/JP00/05833

13.09.00

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

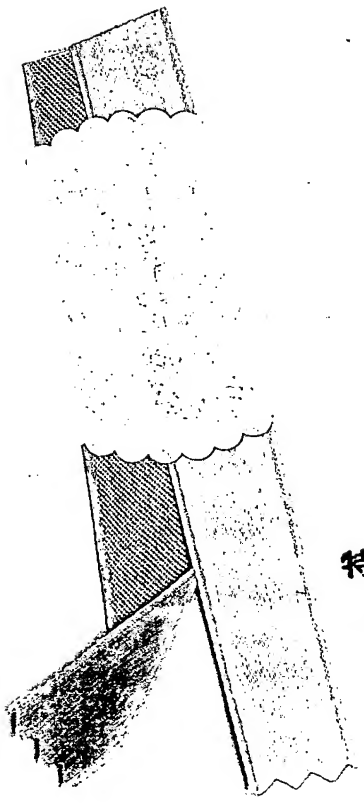
出願年月日
Date of Application: 1999年 8月30日

出願番号
Application Number: 平成11年特許願第243741号

JP 00/05833

出願人
Applicant (s): 富士通株式会社
株式会社日立製作所
日本コロムビア株式会社
三洋電機株式会社

4



2000年10月20日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特2000-3085322

【書類名】　特許願

【整理番号】　1990902

【提出日】　平成11年 8月30日

【あて先】　特許庁長官殿

【国際特許分類】　H04M 11/08

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　畑中　正行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　蒲田　順

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　畠山　卓久

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　長谷部　高行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　東京都小平市上水本町５丁目２０番１号　株式会社日立製作所　半導体グループ内

【氏名】　利根川　忠明

【発明者】
【住所又は居所】　東京都港区赤坂四丁目１４番１４号　日本コロムビア株式会社内
【氏名】　穴澤　健明
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　日置　敏昭
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　金森　美和
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　堀　吉宏
【特許出願人】
【識別番号】　000005223
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】　富士通株式会社
【特許出願人】
【識別番号】　000005108
【住所又は居所】　東京都千代田区神田駿河台４丁目６番地
【氏名又は名称】　株式会社日立製作所
【特許出願人】
【識別番号】　000004167
【住所又は居所】　東京都港区赤坂四丁目１４番１４号
【氏名又は名称】　日本コロムビア株式会社

【特許出願人】
【識別番号】 000001889
【住所又は居所】 大阪府守口市京阪本通２丁目５番５号
【氏名又は名称】 三洋電機株式会社

【代理人】
【識別番号】 100064746
【弁理士】
【氏名又は名称】 深見　久郎

【選任した代理人】
【識別番号】 100085132
【弁理士】
【氏名又は名称】 森田　俊雄

【選任した代理人】
【識別番号】 100091409
【弁理士】
【氏名又は名称】 伊藤　英彦

【選任した代理人】
【識別番号】 100096781
【弁理士】
【氏名又は名称】 堀井　豊

【手数料の表示】
【予納台帳番号】 008693
【納付金額】 21,000円

【提出物件の目録】
【物件名】 明細書　1
【物件名】 図面　1
【物件名】 要約書　1
【プルーフの要否】 要

【書類名】　明細書

【発明の名称】　記録装置

【特許請求の範囲】

【請求項１】　暗号化コンテンツデータを再生出力する再生装置に対して着脱可能であって、前記暗号化コンテンツデータを受けて記録するための記録装置であって、

外部との間でデータの授受を可能とするためのデータ入出力部と、

前記データ入出力部からの前記暗号化コンテンツデータを格納するための第１の記憶部と、

前記記録装置のユーザを識別するための第１のユーザ特定データを保持するためのユーザ情報保持部と、

外部から与えられるユーザ情報と前記第１のユーザ特定データとの比較結果に応じて外部からの指示により更新可能な保護情報を保持する保護情報保持部と、

前記記録装置の動作を制御するための制御部とを備え、

前記制御部は、前記保護情報に基づいて、外部からの前記第１の記憶部に保持された前記暗号化コンテンツデータに対するアクセスを制限する、記録装置。

【請求項２】　前記制御部は、外部から与えられるユーザ情報と前記第１のユーザ特定データとが一致する場合に、前記ユーザ特定データの変更を可能とする、請求項１記載の記録装置。

【請求項３】　前記制御部は、前記ユーザ情報保持部に前記第１のユーザ特定データが未登録の場合に、前記保護情報の変更および前記ユーザ特定データの変更を可能とする、請求項２記載の記録装置。

【請求項４】　前記保護情報保持部は、

前記保護情報のうち、前記記録装置自体に対するアクセスの制限に対する第１の保守情報を保持する第１の保守情報保持部を含み、

前記制御部は、前記第１の保守情報に応じて、前記第１の記憶部に対して、新たな暗号化コンテンツデータの追記を禁止する、請求項１記載の記録装置。

【請求項５】　前記保護情報保持部は、

前記保護情報のうち、前記記録装置自体に対するアクセスの制限に対する第１

の保守情報を保持する第１の保守情報保持部を含み、

前記制御部は、前記第１の保守情報に応じて、前記第１の記憶部に対して、新たな暗号化コンテンツデータの消去を禁止する、請求項１記載の記録装置。

【請求項６】　前記保護情報保持部は、

前記保護情報のうち、前記暗号化コンテンツデータごとのアクセスの制限に対する第２の保守情報を保持する第２の保守情報保持部をさらに含み、

前記制御部は、前記第１および第２の保守情報に応じて、前記第１の記憶部に保持され、前記第２の保守情報に対応する暗号化コンテンツデータの消去を禁止する、請求項５記載の記録装置。

【請求項７】　前記保護情報保持部は、

前記保護情報のうち、前記暗号化コンテンツデータごとのアクセスの制限に対する第２の保守情報を保持する第２の保守情報保持部を含み、

前記制御部は、前記第２の保守情報に応じて、前記第１の記憶部に保持され、前記第２の保守情報に対応する暗号化コンテンツデータの消去を禁止する、請求項１記載の記録装置。

【請求項８】　前記制御部は、外部から前記暗号化コンテンツデータの再生動作が指示された場合、前記第１の記憶部を制御して、前記第２の保守情報に応じて、前記第１の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項６または７記載の記録装置。

【請求項９】　前記制御部は、外部から与えられるユーザ情報と前記第１のユーザ特定データとが一致する場合に、前記第１の記憶部を制御して、前記第２の保守情報に応じて、前記第１の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項８記載の記録装置。

【請求項１０】　前記制御部は、前記ユーザ情報保持部に前記第１のユーザ特定データが未登録の場合に、前記第１の記憶部を制御して、前記第２の保守情報に応じて、前記第１の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項８記載の記録装置。

【請求項１１】　前記制御部は、外部から与えられるユーザ情報と前記第１のユーザ特定データとが一致する場合に、前記第１および第２の保守情報のうち

、少なくとも１つの保守情報を書きかえることを許可する、請求項４～１０のいずれか１項に記載の記録装置。

【請求項１２】　前記制御部は、前記ユーザ情報保持部に前記第１のユーザ特定データが未登録の場合に、前記第１および第２の保守情報のうち、少なくとも１つの保守情報を書きかえることを許可する、請求項４～１０のいずれか１項に記載の記録装置。

【請求項１３】　前記記録装置は、

前記暗号化コンテンツデータにそれぞれ対応し、前記暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第２の記憶部をさらに備え、

前記制御部は、外部から前記第１の記憶部に保持された前記暗号化コンテンツデータの移動が指示された場合、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データとの比較結果に応じて、前記第２の記憶部を制御して、前記ライセンス情報データを前記データ入出力部に与える、請求項１記載の記録装置。

【請求項１４】　前記記録装置は、

前記暗号化コンテンツデータにそれぞれ対応し、前記暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第２の記憶部をさらに備え、

前記ライセンス情報の各々は、前記暗号化コンテンツデータごとに対応するコンテンツユーザ特定データを含み、

前記制御部は、外部から前記第１の記憶部に保持された前記暗号化コンテンツデータの移動が指示された場合、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データと、前記コンテンツユーザ特定データとの比較結果に応じて、前記第２の記憶部を制御して、前記暗号化コンテンツデータごとに前記ライセンス情報データを前記データ入出力部に与える、請求項１記載の記録装置。

【請求項１５】　前記コンテンツユーザ特定データは、対応する前記暗号化コンテンツデータの配信の際に前記ユーザ情報保持部に保持される前記第１のユ

ーザ特定データである、請求項１４記載の記録装置。

【請求項１６】　前記制御部は、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データとの比較結果に応じて、前記コンテンツユーザ特定データの変更を許可する、請求項１４または１５記載の記録装置。

【請求項１７】　前記第１の記憶部は、半導体メモリであり、

前記記録装置は、メモリカードである、請求項１～１６のいずれか１項に記載の記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、携帯電話機等の端末に対して暗号化して配信された情報を格納して保持するための、メモリカードのなどの記録媒体として機能する記録装置の構成に関するものである。

【０００２】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

【０００４】

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物情報の配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】

【発明が解決しようとする課題】

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作物情報の配信が行なわれた場合、各ユーザは、このようにして配信されたコンテンツデータを何らかの記録媒体に記録して保持することになる。

【０００７】

このような記録媒体としては、たとえばメモリカードのように電気的にデータの書込および消去が可能な媒体が用いられることになる。

【０００８】

この場合、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できるものとすると、著作権者の権利保護が図れない。

【０００９】

それのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なったり、コンテンツデータの移動や消去を自由に行なえることとすると、ユーザ側の権利保護にも支障を来たすことになる。

【００１０】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、音楽データ等の著作物データを格納した記録媒体に保持されたコンテンツデータに対して、ユーザ以外の者が無断で再生、移転消去等を行なうことから保護する機能を備えたデータの記録媒体として機能する記録装置を提供することである。

【００１１】

【課題を解決するための手段】

請求項１記載の記録装置は、暗号化コンテンツデータを再生出力する再生装置に対して着脱可能であって、暗号化コンテンツデータを受けて記録するための記録装置であって、外部との間でデータの授受を可能とするためのデータ入出力部と、データ入出力部からの暗号化コンテンツデータを格納するための第１の記憶部と、記録装置のユーザを識別するための第１のユーザ特定データを保持するためのユーザ情報保持部と、外部から与えられるユーザ情報と第１のユーザ特定データとの比較結果に応じて外部からの指示により更新可能な保護情報を保持する保護情報保持部と、記録装置の動作を制御するための制御部とを備え、制御部は、保護情報に基づいて、外部からの第１の記憶部に保持された暗号化コンテンツデータに対するアクセスを制限する。

【００１２】

請求項２記載の記録装置は、請求項１記載の記録装置の構成に加えて、制御部は、外部から与えられるユーザ情報と第１のユーザ特定データとが一致する場合に、ユーザ特定データの変更を可能とする。

【００１３】

請求項３記載の記録装置は、請求項２記載の記録装置の構成に加えて、制御部は、ユーザ情報保持部に第１のユーザ特定データが未登録の場合に、保護情報の変更およびユーザ特定データの変更を可能とする。

【００１４】

請求項４記載の記録装置は、請求項１記載の記録装置の構成に加えて、保護情報保持部は、保護情報のうち、記録装置自体に対するアクセスの制限に対する第１の保守情報を保持する第１の保守情報保持部を含み、制御部は、第１の保守情報に応じて、第１の記憶部に対して、新たな暗号化コンテンツデータの追記を禁止する。

【００１５】

請求項５記載の記録装置は、請求項１記載の記録装置の構成に加えて、保護情報保持部は、保護情報のうち、記録装置自体に対するアクセスの制限に対する第１の保守情報を保持する第１の保守情報保持部を含み、制御部は、第１の保守情報に応じて、第１の記憶部に対して、新たな暗号化コンテンツデータの消去を禁

止する。

【００１６】

請求項６記載の記録装置は、請求項５記載の記録装置の構成に加えて、保護情報保持部は、保護情報のうち、暗号化コンテンツデータごとのアクセスの制限に対する第２の保守情報を保持する第２の保守情報保持部をさらに含み、制御部は、第１および第２の保守情報に応じて、第１の記憶部に保持され、第２の保守情報に対応する暗号化コンテンツデータの消去を禁止する。

【００１７】

請求項７記載の記録装置は、請求項１記載の記録装置の構成に加えて、保護情報保持部は、保護情報のうち、暗号化コンテンツデータごとのアクセスの制限に対する第２の保守情報を保持する第２の保守情報保持部を含み、制御部は、第２の保守情報に応じて、第１の記憶部に保持され、第２の保守情報に対応する暗号化コンテンツデータの消去を禁止する。

【００１８】

請求項８記載の記録装置は、請求項６または７記載の記録装置の構成に加えて、制御部は、外部から暗号化コンテンツデータの再生動作が指示された場合、第１の記憶部を制御して、第２の保守情報に応じて、第１の記憶部に保持された暗号化コンテンツデータをデータ入出力部に与えることを禁止する。

【００１９】

請求項９記載の記録装置は、請求項８記載の記録装置の構成に加えて、制御部は、外部から与えられるユーザ情報と第１のユーザ特定データとが一致する場合に、第１の記憶部を制御して、第２の保守情報に応じて、第１の記憶部に保持された暗号化コンテンツデータをデータ入出力部に与えることを禁止する。

【００２０】

請求項１０記載の記録装置は、請求項８記載の記録装置の構成に加えて、制御部は、ユーザ情報保持部に第１のユーザ特定データが未登録の場合に、第１の記憶部を制御して、第２の保守情報に応じて、第１の記憶部に保持された暗号化コンテンツデータをデータ入出力部に与えることを禁止する。

【００２１】

請求項１１記載の記録装置は、請求項４～１０のいずれか１項に記載の記録装置の構成に加えて、制御部は、外部から与えられるユーザ情報と第１のユーザ特定データとが一致する場合に、第１および第２の保守情報のうち、少なくとも１つの保守情報を書きかえることを許可する。

【００２２】

請求項１２記載の記録装置は、請求項４～１０のいずれか１項に記載の記録装置の構成に加えて、制御部は、ユーザ情報保持部に第１のユーザ特定データが未登録の場合に、第１および第２の保守情報のうち、少なくとも１つの保守情報を書きかえることを許可する。

【００２３】

請求項１３記載の記録装置は、請求項１に記載の記録装置の構成に加えて、記録装置は、暗号化コンテンツデータにそれぞれ対応し、暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第２の記憶部をさらに備え、制御部は、外部から第１の記憶部に保持された暗号化コンテンツデータの移動が指示された場合、外部から与えられる再生装置に対する第２のユーザ特定データと、ユーザ情報保持部に保持される第１のユーザ特定データとの比較結果に応じて、第２の記憶部を制御して、ライセンス情報データをデータ入出力部に与える。

【００２４】

請求項１４記載の記録装置は、請求項１に記載の記録装置の構成に加えて、記録装置は、暗号化コンテンツデータにそれぞれ対応し、暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第２の記憶部をさらに備え、ライセンス情報の各々は、暗号化コンテンツデータごとに対応するコンテンツユーザ特定データを含み、制御部は、外部から第１の記憶部に保持された暗号化コンテンツデータの移動が指示された場合、外部から与えられる再生装置に対する第２のユーザ特定データと、ユーザ情報保持部に保持される第１のユーザ特定データと、コンテンツユーザ特定データとの比較結果に応じて、第２の記憶部を制御して、暗号化コンテンツデータごとにライセンス情報データをデータ入出力部に与える。

【００２５】

請求項１５記載の記録装置は、請求項１４に記載の記録装置の構成に加えて、コンテンツユーザ特定データは、対応する暗号化コンテンツデータの配信の際にユーザ情報保持部に保持される第１のユーザ特定データである。

【００２６】

請求項１６記載の記録装置は、請求項１４または１５に記載の記録装置の構成に加えて、制御部は、外部から与えられる再生装置に対する第２のユーザ特定データと、ユーザ情報保持部に保持される第１のユーザ特定データとの比較結果に応じて、コンテンツユーザ特定データの変更を許可する。

【００２７】

請求項１７記載の記録装置は、請求項１から１６のいずれか１項に記載の記録装置の構成に加えて、第１の記憶部は、半導体メモリであり、記録装置は、メモリカードである。

【００２８】

【発明の実施の形態】

［実施の形態１］

［配信データの受信端末（携帯電話）の構成］

図１は、本発明の記録媒体が使用される情報配信システムにおいて、情報の配信を受けるための端末である携帯電話機１００の構成を説明するための概略ブロック図である。

【００２９】

図１を参照して、携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機１００からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６と、携帯電話機１００の所有者を識別するためのユーザＩＤデータＵｓｅｒ－ＩＤｈを保持するユーザＩＤ保持部１１０７と、外部からの指示を携帯電話機１００に与えるためのタ

ッチキー部１１０８と、コントローラ１１０６から出力される情報をユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データバスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２と、外部との間でデータの授受を行なうためのコネクタ１１２０と、コネクタ１１２０からのデータをデータバスＢＳ２に与え得る信号に変換し、または、データバスＢＳ２からのデータをコネクタ１１２０に与え得る信号に変換するための外部インターフェイス部１１２２とを備える。

【００３０】

ここで、たとえば、ユーザＩＤデータは、ユーザの携帯電話機の電話番号、またはユーザ自身が設定したデータ、あるいはその両者の組合せのデータ等を含む。

【００３１】

携帯電話機１００は、さらに、音楽サーバから供給される暗号化コンテンツデータを格納するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインターフェイス１２００と、メモリカード１１０からの暗号化されたコンテンツデータとこの暗号化されたコンテンツデータを復号するためのコンテンツキーＫｃとを受けて、音楽データを再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２と、デジタルアナログ変換部１５１２の出力を受けて、たとえば、ヘッドホーン（図示せず）と接続するための接続端子１５１４とを含む。

【００３２】

なお、説明の簡略化のため本発明の記録媒体中に格納された音楽データの配信および再生に係るブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、図１では一部割愛されている。

【００３３】

［メモリカードの構成］

図２は、図１に示したメモリカード１１０の構成を説明するための概略ブロック図である。

【００３４】

以下では、携帯電話機１００に装着されるメモリカード１１０に固有な秘密復号キーをキーＫｍｃ（１）とする。一方、他のメモリカードに固有な秘密復号キーをキーＫｍｃ（ｎ）（ｎ：自然数）とする。ここで、自然数ｎは、メモリカードを区別するためのものである。すなわち、キーＫｍｃ（ｎ）は、メモリカードごとに異なるものである。

【００３５】

また、これに対応して、秘密復号キーＫｍｃ（１）で復号可能な暗号化を提供し、キーＫｍｃ（１）とは非対称な、言い換えると同一の秘密復号キーＫｍｃ（１）に対して複数個存在し得る公開暗号化キーを公開暗号化キーＫＰｍｃ（１）と称し、同様にして、秘密復号キーＫｍｃ（ｎ）で復号可能な暗号化を提供し、キーＫｍｃ（ｎ）とは非対称な公開暗号化キーを公開暗号化キーＫＰｍｃ（ｎ）と称することとする。

【００３６】

図２を参照して、メモリカード１１０は、インターフェイス１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、公開暗号化キーＫＰｍｃ（１）を保持し、データバスＢＳ３に公開暗号化キーＫＰｍｃ（１）を出力するためのＫＰｍｃ（１）保持部１４０５と、端子１２０２およびデータバスＢＳ３を介して他のメモリカードから送信された公開暗号化キーＫＰｍｃ（ｎ）に基づいて、入力されたデータを暗号化するための暗号化処理部１４１４と、秘密復号キーＫｍｃ（１）を保持するためのＫｍｃ（１）保持部１４１５と、データバスＢＳ３から与えられるデータを受けて、Ｋｍｃ（１）保持部１４１５からの秘密復号キーＫｍｃ（１）に基づいて復号処理をするための復号処理部１４１６と、メモリカード１１０の動作を制御するためのコントローラ１４２０と、データバスＢＳ３を介して、配信される暗号化コンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）と、暗号化されたコンテンツキーおよびライセンス情報データ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）を格納し保持するためのメモリ１４１

２とを含む。メモリ１４１２は、いわゆる半導体メモリであって、とくに限定されないが、たとえば、不揮発性メモリであるフラッシュメモリ等を用いることが可能である。

【００３７】

ここで、記号［Ｘ］Ｙは、復号キーＹで復号可能な暗号化処理でデータＸが暗号化されていることを表わす。

【００３８】

メモリカード１１０は、さらに、メモリカード１１０についてのユーザに関する情報であるユーザＩＤデータを保持するためのユーザＩＤ保持部１５３０と、メモリカード１１０に対する保守情報を保持するための第１の保守情報保持部１５２０と、復号処理部１４１６から出力される復号化されたデータを暗号化処理部１４１４およびコントロール１４２０等へ伝達するためのデータバスＢＳ５と、コンテンツデータＤｃ（ｉ）に対応し、当該コンテンツデータの再生回数の制限等の再生権に関する情報やコンテンツデータの所有権等を示すライセンス情報データＬｉｃｅｎｓｅ（ｉ）を保持するためのライセンス情報保持部１５００と、コンテンツデータＤｃ（ｉ）（ｉ：自然数）ごとに設定されるコンテンツ保守情報を保持するための第２の保守情報保持部１５４０とを備える。

【００３９】

なお、上述した構成において、コンテンツデータＤｃ（ｉ）やコンテンツキーデータＫｃ（ｉ）、ライセンス情報データＬｉｃｅｎｓｅ（ｉ）等の自然数ｉは、各コンテンツデータごとにこれらのデータが異なることを表現している。

【００４０】

また、図２において実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。

【００４１】

このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）と呼ばれる。

【００４２】

もちろん、メモリ１４１２も含めて、モジュールＴＲＭに組込まれる構成としてもよい。しかしながら、図２に示したような構成とすることで、メモリ１４１２中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１２中のデータのみでは、音楽データ等のコンテンツデータを再生することは不可能である。このため、高価なタンパーレジスタンスモジュール内にメモリ１４１２を設ける必要がないので、製造コストが低減されるという利点がある。

【００４３】

ここで、メモリカード１１０に対する動作として、メモリ１４１２中に保持されているコンテンツデータをそのままの状態に保持して、さらに異なるコンテンツデータを追加して記録する動作を「追記」と呼び、メモリ１４１２中に含まれるコンテンツデータ等を消去する動作または再生できる状態にする動作を「消去」と呼ぶ。

【００４４】

以下の表１は、図２に示した第１の保守情報保持部１５２０中に保持される上記追記動作および消去動作を制御するための追記フラグおよびメディア消去フラグの状態と、それに対応するメモリカードの動作状態との関係を説明する表である。

【００４５】

【表１】

メディア単位の管理

保守情報＼値	1	0
追記フラグ	追記可能	追記禁止
メディア消去フラグ	消去可能	消去禁止

【００４６】

すなわち、第１の保守情報保持部１５２０中に保持される追記フラグが「１」である場合は、メモリ１４１２中に保持されたコンテンツデータに加えて、さらに新たなコンテンツデータの書込を行なうことが許可されており、追記フラグが「０」である場合はこのような追記動作が禁止されている。

【００４７】

一方、第１の保守情報保持部１５２０に保持されるメディア消去フラグが「１」である場合は、このメモリカード１１０に対してメモリ１４１２に保持されたデータを外部からの指示に応じて消去することが可能であるのに対し、メディア消去フラグが「０」である場合はこのような消去動作は一切禁止されている。

【００４８】

一方、メモリカード１１０は、外部から与えられる指示に応じて、コントローラ１４２０の制御の下、メモリ１４１２中に保持された各コンテンツデータごとの処理を制御するための保守情報を第２の保守情報保持部１５４０が保持している。

【００４９】

以下では、コンテンツデータごとの再生処理を特に「コンテンツ再生」と呼び、コンテンツデータごとの消去動作を特に「コンテンツ消去」と呼ぶことにする。

【００５０】

表２は、第２の保守情報保持部１５４０が保持するデータと、メモリカード１１０のコントローラ１４２０による制御状態との関係を示す表である。

【００５１】

【表２】

コンテンツデータ単位の管理

保守情報＼値	1	0
コンテンツ再生フラグ	再生可能	再生禁止*
コンテンツ消去フラグ	消去可能	消去禁止

＊）携帯電話機におけるユーザIDが同一の場合は再生可能

【００５２】

すなわち、第２の保守情報保持部１５４０が各コンテンツデータごとに対応して保持するコンテンツ再生フラグが「１」である場合は、対応するコンテンツデータは再生可能状態であり、コンテンツ再生フラグが「０」である場合は原則として当該コンテンツデータの再生は禁止される。

【００５３】

ただし、以下に説明するようにコンテンツ再生フラグが「０」である場合であっても、携帯電話機１００のユーザＩＤデータとメモリカードのユーザＩＤデータとが一致する場合は、当該コンテンツデータの再生動作が許可される。

【００５４】

一方、第２の保守情報保持部１５４０においてコンテンツデータごとに対応して保持されるコンテンツ消去フラグが「１」である場合は、当該コンテンツデータに関しては消去動作が許可されており、コンテンツ消去フラグが「０」である場合は当該コンテンツデータに対する消去動作が禁止されている。

【００５５】

以上のように、メモリカードごとおよびコンテンツデータごとに予め保守情報を設定しておくことで、正規ユーザ以外の者がメモリカード１１０内に保持されたコンテンツデータに対する処理を行なうことを制限し、当該メモリカードのユーザが正当な対価の下に購入したコンテンツデータを保護することが可能となる。

【００５６】

［配信システムの全体構成］

図３は、本発明の記録媒体が用いられる情報配信システムの全体構成を概略的に説明するための概念図である。

【００５７】

なお、以下では携帯電話網を介して、デジタル音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物情報データ、たとえば画像データ等の著作物データを、メモリ等に配信した上でアクセスするあらゆる場合にも適用することが可能なものである。

【００５８】

また、データの配信の方法も携帯電話網による配信に限られるものではなく、たとえば、他の情報通信網を介した配信や、多数のコンテンツデータを蓄えたコンテンツデータ販売機を街頭に設置し、ユーザは、携帯電話機のインターフェースを介して、または、メモリカードに直接にこのコンテンツデータ販売機からコンテンツデータを購入することで、著作物データを入手する構成としても良い。

【００５９】

さらに、暗号化されたコンテンツデータを再生する機器も、携帯電話機に限定されることなく、たとえば、上記メモリカードに対応した専用の再生装置であってもよい。

【００６０】

図３を参照して、著作権の存在する音楽情報を管理する配信サーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、音楽データを配信するための配信キャリアである携帯電話会社２０に、このような暗号化コンテンツデータを与える。一方、認証サーバ１２は、音楽データの配信を求めてアクセスしてきたユーザが正規のユーザであるか否かの認証を行う。

【００６１】

携帯電話会社２０は、自己の携帯電話網を通じて、各ユーザからの配信要求（

配信リクエスト）を配信サーバ１０に中継する。配信サーバ１０は、配線リクエストがあると、認証サーバ１２によりユーザが正規のユーザであることを確認し、要求された音楽情報をさらに暗号化したうえで、携帯電話会社２０の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

【００６２】

図３においては、たとえば、携帯電話ユーザ１の携帯電話機１００には、携帯電話機１００により受信された暗号化された音楽データを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機１００中の音楽再生部（図示せず）に与えるために、図２において説明したような着脱可能なメモリカード１１０が装着される構成となっている。

【００６３】

さらに、たとえばユーザ１は、携帯電話機１００に接続したヘッドホン１２０等を介してこのような再生された音楽データを聴取することが可能である。

【００６４】

以下では、このような配信サーバ１０と認証サーバ１２と配信キャリア（携帯電話会社）２０とを併せて、音楽サーバ３０と総称することにする。

【００６５】

また、このような音楽サーバ３０から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

【００６６】

このような構成とすることで、まず、メモリカード１１０を購入していない正規のユーザでないものは、音楽サーバ３０からの配信データを受取って再生することが困難な構成となる。

【００６７】

しかも、配信キャリア２０において、たとえば１曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信するたびに発生する著作権料を、配信キャリア２０が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００６８】

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【００６９】

このとき、たとえばメモリカード１１２を有するユーザ２が、自己の携帯電話機１０２により、音楽サーバ３０から直接音楽データの配信を受けることは可能である。しかしながら、相当量の情報量を有する音楽データ等をユーザ２が直接音楽サーバ３０から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該音楽データの配信を受けているユーザ１から、その音楽情報をコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

【００７０】

図３に示した例では、ユーザ１が受信した音楽データを、デジタル音楽データそのものおよび当該音楽データを再生可能とするために必要な情報とともに、ユーザ２に対してコピーさせる場合を音楽データの「移動」と呼ぶ。この場合、ユーザ１は、再生のために必要な情報（再生情報）ごとユーザ２にコピーさせるため、情報の移動を行なった後には、ユーザ１においては音楽データの再生を行なうことを不可能とする必要がある。ここで、「再生情報」とは、後に説明するように、上記所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なコンテンツキーと、著作権保護に関わる情報であるライセンスＩＤデータやユーザＩＤデータ等のライセンス情報とを意味する。

【００７１】

これに対して、音楽データ（コンテンツデータ）のみを暗号化されたままの状態で、ユーザ２にコピーさせることを音楽情報の「複製」と呼ぶこととする。

【００７２】

この場合、ユーザ２の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされないので、ユーザ２は、コンテンツデータを得ただけでは、音楽情報を再生させることができない。したがって、ユーザ２が、このような音楽情報の再生を望む場合は、改めて音楽サーバ３０からコンテンツ

データの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよいため、ユーザ２が直接音楽サーバ３０からすべての情報の配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

【００７３】

たとえば、携帯電話機１００および１０２が、ＰＨＳ（Personal Handy Phone）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ１からユーザ２への一括した情報の移転（移動）や、コンテンツデータのみの転送（複製）を行なうことが可能である。

【００７４】

［暗号／復号キーの構成］

図４は、図３に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【００７５】

まず、図３に示した構成において、メモリカード１１０内のデータ処理を管理するための鍵としては、メモリカードごとに異なる公開暗号化鍵ＫＰｍｃ（ｎ）と、公開暗号化鍵ＫＰｍｃ（ｎ）により暗号化されたデータを復号するための秘密復号鍵Ｋｍｃ（ｎ）とがある。

【００７６】

ここで、鍵Ｋｍｃ（ｎ）や鍵ＫＰｍｃ（ｎ）の表記中の自然数ｎは、各メモリカードを区別するための番号を表わす。

【００７７】

したがって、メモリカードにおける配信データの授受にあたっては、後に説明するように２つの暗号鍵Ｋｍｃ（ｎ）、ＫＰｍｃ（ｎ）が用いられることになる。

【００７８】

また、メモリカードは、メモリカードのユーザを識別するためのユーザＩＤデータＵｓｅｒ－ＩＤｍを保持している。一方、携帯電話は、携帯電話機のユーザを識別するためのユーザＩＤデータＵｓｅｒ－ＩＤｈを保持している。

【００７９】

さらに、配信されるべきデータについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるＫｃ（以下、ライセンスキーと呼ぶ）があり、この共通鍵Ｋｃにより暗号化されたコンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンス情報データＬｉｃｅｎｓｅ（ｉ）等が存在する。

【００８０】

このような構成とすることで、ライセンスＩＤデータに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザＩＤデータを用いることで、コンテンツデータの配信を正規に受けたユーザの保護、たとえば、ユーザの許可無く、配信されたコンテンツデータが消去されることを防止するなどの制御を行なうことが可能である。

【００８１】

配信データにおけるコンテンツデータＤｃは、上述のとおり、たとえば音楽情報データであり、このコンテンツデータをライセンスキーＫｃで復号化可能なデータを、暗号化コンテンツデータ［Ｄｃ］Ｋｃと呼ぶ。

【００８２】

［配信サーバ１０の構成］

図５は、図３に示した配信サーバ１０の構成を示す概略ブロック図である。

【００８３】

配信サーバ１０は、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したデータや、ライセンスＩＤデータ等の配信情報を保持するための配信情報データベース３０４と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース３０２と、配信情報データベース３０４および課金データベース３０２からのデータをデータバスＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００８４】

データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１２と、携帯電話通信網を介して、通信装置３５０により受信されたメモリカードｎからの公開暗号化キーＫＰｍｃ（ｎ）を受取り、配信制御部３１２から与えられる暗号化コンテンツデータを、この公開暗号化キーＫＰｍｃ（ｎ）で更に暗号化してデータバスＢｓ１に与えるための暗号化処理部３２０とを備える。

【００８５】

通信装置３５０は、このようにして暗号化処理部３２０により暗号化されたコンテンツデータを後に説明するように通信網と、配信キャリア２０と、携帯電話網とを介して携帯電話機端末１００等に送信する。

【００８６】

［実施の形態１の配信処理（保守情報がない場合）］

図６は、図１、図２、図３および図５で説明した情報配信システムにおけるコンテンツデータの配信動作を説明するためのフローチャートである。

【００８７】

図６においては、ユーザ１が、メモリカード１１０を用いることで、音楽サーバ３０から音楽データの配信を受ける場合の動作を説明している。

【００８８】

まず、配信動作が開始されると、ユーザ１の携帯電話機１００からユーザによりキーボード１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【００８９】

配信サーバ３０は、携帯電話機１００からの配信リクエストを受理すると、携帯電話機１００に対して、公開暗号化キーＫＰｍｃ（１）の送信要求を出力する（ステップＳ１０２）。

【００９０】

携帯電話機１００は、サーバ３０からの公開暗号化キーＫＰｍｃ（１）の送信要求を受信すると（ステップＳ１０４）、カード１１０に対して転送し、カード

１１０は、これに応じて、公開暗号化キーＫＰｍｃ（１）を携帯電話機１００に対して出力する（ステップＳ１０６）。

【００９１】

携帯電話機１００は、メモリカード１１０からのキーデータＫＰｍｃ（１）を受けると、サーバ３０に対してこれを送信する（ステップＳ１０８）。

【００９２】

配信サーバ１０は、携帯電話機１００からのキーＫＰｍｃ（１）を受信すると（ステップＳ１１０）、配信情報データベース３０４からの情報をもとにライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ１１２）。

【００９３】

続いて、配信サーバ３０は、配信情報データベース３０４から、コンテンツキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを取得する（ステップＳ１１４）。

【００９４】

続いて配信サーバ３０は、携帯電話機１００へ暗号化コンテンツデータ［Ｄｃ］Ｋｃ

を送信する（ステップＳ１１６）。

【００９５】

携帯電話機１００は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１１８）、メモリカード１１０に転送し、メモリカード１１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２にこのまま格納する（ステップＳ１２０）。

【００９６】

一方、サーバ３０は、コンテンツキーＫｃを配信情報データベースより取得し（ステップＳ１２２）、メモリカード１１０から送信された公開暗号化キーＫＰｍｃ（１）によりこのコンテンツキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅを暗号化して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を生成する（ステップＳ１２４）。

【００９７】

配信サーバ１０から携帯電話機１００へデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）が送信され（ステップＳ１２６）、携帯電話機１００がこれを受信すると（ステップＳ１２８）、メモリカード１１０は携帯電話機１００からこのデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を受取ってメモリ１４１２に格納する（ステップＳ１３０）。

【００９８】

続いて、メモリカード１１０は、秘密復号キーＫｍｃ（１）によりデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を復号し、抽出されたライセンスデータＬｉｃｅｎｓｅをライセンス情報保持部１５００に格納する（ステップＳ１３２）。

【００９９】

ライセンス情報データＬｉｃｅｎｓｅのライセンス情報保持部１５００への格納の終了に応じて、携帯電話機１００から配信サーバ３０に対して配信受理が送信される（ステップＳ１３４）。

【０１００】

サーバ３０は配信受理を受信すると（ステップＳ１３６）、課金データベースに配信情報を記録する（ステップＳ１３８）。

【０１０１】

以上のような処理により、サーバ３０からメモリカード１１０に対してコンテンツデータ、ライセンス情報データＬｉｃｅｎｓｅおよびコンテンツキーＫｃが配信される。

【０１０２】

［実施の形態１の再生処理（保守情報による保護のない場合）］

図７は、携帯電話機１００内において、メモリカード１１０に保持された暗号化コンテンツデータから、音楽データを復号化し、音楽として外部に出力するための再生処理を説明するためのフローチャートである。以下の説明では、まず、上述したような保守情報により再生処理に保護がかかっていない状態の処理のフローを説明する。

【０１０３】

なお、以下では、暗号化されたデータを復号化した状態、すなわち、本来の状

態に復帰したデータを「平文データ」と呼ぶことにする。

【０１０４】

図７を参照して、再生処理が開始されると、まず携帯電話機１００のキーボード１１０８等からユーザ１の指示により、再生リクエストがメモリカード１１０に対して出力される（ステップＳ２００）。

【０１０５】

カード１１０においては、この再生リクエストに応じて、コントローラ１４２０は、ライセンス情報保持部１５００に保持されるライセンス情報データに基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップＳ２０２）、再生可能と判断した場合はメモリ１４１２内のライセンス情報データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を秘密復号キーＫｍｃ（１）により復号する（ステップＳ２０４）。

【０１０６】

一方、コントローラ１４２０が再生不可能と判断した場合は、処理が終了する（ステップＳ２１６）。

【０１０７】

再生可能と判断され、カード１１０において、メモリ１４１２内のデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）が復号処理されることで、コンテンツキーＫｃが抽出されると（ステップＳ２０４）、カード１１０からコンテンツキーＫｃが携帯電話機１００に対して出力される（ステップＳ２０６）。

【０１０８】

携帯電話機１００が、コンテンツキーＫｃを受理すると（ステップＳ２０８）、続いて、メモリカード１１０からはメモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］ｋｃが携帯電話機１００に対して出力される（ステップＳ２１０）。

【０１０９】

携帯電話機１００においては、音楽再生部１５０８が、メモリカード１１０から与えられたコンテンツキーＫｃにより暗号化コンテンツデータ［Ｄｃ］Ｋｃを復号処理して、平文化された音楽データを生成する（ステップＳ２１２）。

【０１１０】

音楽再生部１５０８からの出力は混合部１５１０を経由して、デジタルアナログ変換処理部１５１２に伝達され、デジタルアナログ変換処理部１５１２から平文化音楽データがアナログ音楽信号として再生出力されて（ステップＳ２１４）、再生処理が終了する（ステップＳ２１６）。

【０１１１】

以上の処理により、配信サーバ１０からメモリカード１１０に対して配信された暗号化コンテンツキーに基づいて、音楽の再生処理が行なわれることになる。

【０１１２】

［実施の形態１の移動処理（保守情報による保護のない場合）］

図８および図９は、２つのメモリカード間において、コンテンツデータおよびキーデータの移動を行なう処理を説明するためのフローチャートである。

【０１１３】

また、図８および図９においても、まず、保守情報による保護がない場合について説明する。

【０１１４】

まず、携帯電話機１０２が送信側であり、携帯電話機１００が受信側であるものとする。また、携帯電話機１０２にも、メモリカード１１０と同様の構成を有するメモリカード１１２が装着されているものとする。

【０１１５】

移動動作が開始されると、携帯電話機１０２におけるキータッチ部１１０８等とから、ユーザ２により移動リクエストが指示され（ステップＳ３００）、携帯電話機１０２から携帯電話機１００へ公開暗号化キーＫＰｍｃ（１）の送信要求が送信される（ステップＳ３０２）。

【０１１６】

携帯電話機１００が公開暗号化キーＫＰｍｃ（１）の送信要求を受信すると（ステップＳ３０４）、メモリカード１１０は、これに応じて、公開暗号化キーＫＰｍｃ（１）を出力する（ステップＳ３０６）。

【０１１７】

携帯電話機１００は、メモリカード１１０からの公開暗号化キーＫＰｍｃ（１

）を受取って携帯電話機１０２に対して出力し（ステップＳ３０８）、携帯電話機１０２は、キーＫＰｍｃ（１）を受信すると（ステップＳ３１０）、これをメモリカード１１２に転送する。

【０１１８】

メモリカード１１２は、キーデータＫＰｍｃ（１）を受理すると（ステップＳ３１２）、メモリカード１１２のメモリ１４１２中の暗号化コンテンツデータ［Ｄｃ］Ｋｃを携帯電話機１０２に対して出力する（ステップＳ３１４）。

【０１１９】

携帯電話機１０２から暗号化コンテンツデータ［Ｄｃ］Ｋｃが携帯電話機１００に対して送信され（ステップＳ３１６）、携帯電話機１００がこれを受信すると（Ｓ３１８）、転送された暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリカード１１０は、メモリカード１１０のメモリ１４１２に格納する（ステップＳ３２０）。

【０１２０】

続いて、メモリカード１１２においては、メモリカード１１２のメモリ１４１２内の暗号化されたライセンス情報データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（２）を秘密復号キーＫｍｃ（２）により復号する（ステップＳ３２２）。

【０１２１】

続いて、メモリカード１１２は、メモリカード１１０から送信されたメモリカード１１０の公開暗号化キーＫＰｍｃ（１）によりコンテンツキーデータＫｃおよびライセンス情報データＬｉｃｅｎｓｅを暗号化して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を生成し（ステップＳ３２４）、これを携帯電話機１０２に対して出力する（ステップＳ３２６）。

【０１２２】

続いて図９を参照して、携帯電話機１０２から携帯電話機１００へ、暗号化されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）が送信されると（ステップＳ３２８）、携帯電話機１００はこれを受信して（ステップＳ３３０）、メモリカード１１０は、転送されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を受理する（ステップＳ３３２）。

【０１２３】

続いて、メモリカード１１０は、この受信したデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）をメモリカード１１０のメモリ１４１２に格納し（ステップＳ３３４）、続いて、秘密復号キーＫｍｃ（１）によって、このデータを復号して、抽出されたライセンス情報データＬｉｃｅｎｓｅをライセンス情報保持部１５００に格納する（ステップＳ３３６）。

【０１２４】

メモリカード１１０において、ライセンス情報データＬｉｃｅｎｓｅのライセンス情報保持部１５００への格納が完了すると、携帯電話機１００から携帯電話機１０２へ配信受理が送信され（ステップＳ３３８）、携帯電話機１０２において、この配信受理が受信されると（ステップＳ３４０）、メモリカード１１２内のライセンス情報保持部１５００のライセンス情報データＬｉｃｅｎｓｅの消去動作が行なわれる（ステップＳ３４２）。

【０１２５】

このメモリカード１１２内におけるライセンス情報データＬｉｃｅｎｓｅの消去が完了し（ステップＳ３４２）、かつ、メモリカード１１２のメモリ１４１２内のデータ消去を行なうか否かの確認をユーザ２が携帯電話機１０２のキータッチ部１１０８を介して行なうと（ステップＳ３４４）、続いて、メモリカード１１２のコントローラ１４２０はメモリ内のデータ消去を行なうか否かの判断を行ない（ステップＳ３４６）、ステップＳ３４４において、メモリ１４１２内のデータ消去が確認されている場合、メモリカード１１２のメモリ１４１２内のデータ［Ｄｃ］Ｋｃおよび［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（２）の消去動作を行ない（ステップＳ３４８）、処理が終了する（ステップＳ３５０）。

【０１２６】

一方、メモリ内のデータ消去が許可されない場合（ステップＳ３４６）、そのまま処理が終了する（ステップＳ３５０）。

【０１２７】

メモリ内のデータ消去が許可されていない場合においても、メモリカード１１２内のライセンス情報保持部１５００内のライセンス情報データＬｉｃｅｎｓｅ

が消去されているので、メモリカード１１２は、新たにコンテンツキーデータＫｃおよびライセンス情報データＬｉｃｅｎｓｅをサーバ３０から配信してもらい、ライセンス情報保持部１５００にライセンス情報を保持しない限り、暗号化コンテンツデータ［Ｄｃ］Ｋｃの再生処理を行なうことはできない。

【０１２８】

［ユーザＩＤ、保守情報の変更処理］

図１０は、本発明のメモリカード１１０の保守情報（メディア消去フラグ、追記フラグ、コンテンツ再生フラグ、コンテンツ消去フラグ）またはユーザＩＤデータＵｓｅｒ－ＩＤｍの変更指示の処理を説明するためのフローチャートである。

【０１２９】

まず変更処理が開始されると、ユーザは、携帯電話機１００のタッチキー部１０８等から、保守情報またはユーザＩＤデータの変更指示を行なう（ステップＳ４００）。

【０１３０】

続いて、メモリカードに、ユーザＩＤデータが登録されているか否かの判断が行なわれ（ステップＳ４０２）、ユーザＩＤデータが登録されている場合、メモリカード１１０のコントローラ１４２０は、携帯電話機１００のユーザＩＤ保持部１１０７から携帯電話機１００に登録されているユーザＩＤデータＵｓｅｒ－ＩＤｈを入手する（ステップＳ４０４）。

【０１３１】

続いて、コントローラ１４２０は、携帯電話機１００に登録されているユーザＩＤデータＵｓｅｒ－ＩＤｈの値と、メモリカードのユーザＩＤ保持部１５２０に登録されているユーザＩＤデータＵｓｅｒ－ＩＤｍとの比較を行ない（ステップＳ４０６）、一致している場合は、保守情報またはユーザＩＤの変更を行ない（ステップＳ４０８）、処理が終了する（ステップＳ４１２）。ここで、ユーザＩＤデータの変更とは、すでに登録されているユーザＩＤデータの値を別の値に書きかえることであってもかまわないし、また、すでに登録されているユーザＩＤデータの値を消去することであってもかまわない。また、ユーザＩＤを複数個

登録できる場合は、ユーザＩＤデータを追加する構成であっても良い。

【０１３２】

また、この場合、保守情報の変更は、第１の保守情報保持部１５２０中のメディア単位の管理データの変更でもかまわないし、第２の保守情報保持部１５４０中のコンテンツデータ単位の管理データ単位の変更でもかまわない。

【０１３３】

一方、ステップＳ４０２において、メモリカードにユーザＩＤが登録されていない場合、コントローラ１４２０は、携帯電話機に登録されたユーザＩＤ情報との比較を行なうことなく、保守情報またはユーザＩＤデータの変更処理を行ない（ステップＳ４０８）、処理が終了する（ステップＳ４１２）。

【０１３４】

一方、メモリカードにユーザＩＤが登録されている場合において、ステップＳ４０６において、携帯電話機のユーザＩＤとメモリカードのユーザＩＤとが一致しない場合は、コントローラ１４２０から携帯電話機１００に対して変更不可の通知がされ（ステップＳ４１０）、処理が終了する（ステップＳ４１２）。

【０１３５】

携帯電話機１００では、変更不可の通知を受けると、ディスプレイ１１１０等を介して、ユーザに対し変更処理が許可されないことを通知する。

【０１３６】

［再生処理（保守情報の考慮のある場合）］

図１１は、保守情報の考慮のある場合について、本発明のメモリカードのコンテンツデータＤｃ（ｉ）の再生処理を指示した場合のメモリカード１１０の動作を説明するためのフローチャートであり、保守情報の考慮を行なわない場合の図７と対比される図である。

【０１３７】

処理が開始されると、ユーザは携帯電話機１００のタッチキー部１１０８のキー操作等により、複数のコンテンツデータのうちのあるコンテンツデータＤｃ（ｉ）の再生指示を行なう（ステップＳ５００）。

【０１３８】

自然数ｉは、メモリカードに記録された複数の音楽データを区別するものである。

【０１３９】

メモリカード１１０のコントローラ１４２０は、この再生指示に応じて、ライセンス情報保持部１５００中に保持されたコンテンツデータＤｃ（ｉ）に対応するライセンス情報データＬｉｃｅｎｓｅ（ｉ）の内容を確認する（ステップＳ５０２）。たとえば、ライセンス情報データＬｉｃｅｎｓｅ（ｉ）の値により、再生回数が制限されている場合、この制限範囲以内であるならば、再生可能と判断され、処理は次のステップに移行する。

【０１４０】

一方、ライセンス情報データＬｉｃｅｎｓｅ（ｉ）により、再生不可が指定されている場合は、コントローラ１４２０は、携帯電話機１００に対して再生不可の通知を出力し（ステップＳ５１２）、処理が終了する（ステップＳ５２０）。

【０１４１】

再生可能であると判断された場合、続いて、コントローラ１４２０は、コンテンツデータＤｃ（ｉ）に対するコンテンツデータ単位の保守情報を第２の保守情報保持部１５４０に対して照会し、コンテンツ再生フラグの値を確認する（ステップＳ５０４）。当該コンテンツデータＤｃ（ｉ）に対する再生が可能である状態にコンテンツ再生フラグが設定されている場合、コントローラ１４２０に制御されて、復号処理部１４１６は、メモリ１４１２中に保持されている暗号化されたデータ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）を、秘密復号キーＫｍｃ（１）により復号する（ステップＳ５１４）。

【０１４２】

このようにしてコンテンツキーＫｃ（ｉ）が、復号抽出され携帯電話機１００の音楽再生部１５０８に対して出力される（ステップＳ５１６）。

【０１４３】

さらに、メモリ１４１２からは暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）が、携帯電話機１００の音楽再生部１５０８に対して出力され（ステップＳ５１８）、処理が終了する（Ｓ５２０）。

【０１４４】

一方、ステップＳ５０４において、コンテンツ再生フラグのレベルにより、再生禁止が指示されている場合は、続いて、ユーザＩＤ保持部１５２０中にユーザＩＤが登録されているか否かの判断が行なわれる（ステップＳ５０６）、登録されていない場合、処理はステップＳ５１４に進み、コンテンツキーデータＫｃ（ｉ）の復号抽出および暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）の出力が行なわれる。

【０１４５】

これに対して、ユーザＩＤ保持部１５２０中にユーザＩＤが登録されている場合、コントローラ１４２０は、携帯電話機１００のユーザＩＤ保持部１１０７から携帯電話機１００のユーザＩＤデータを取得し（ステップＳ５０８）、携帯電話機１００に登録されたユーザＩＤデータＵｓｅｒ－ＩＤｈと、メモリカードに登録されているユーザＩＤデータＵｓｅｒ－ＩＤｍの値が一致しているか否かの判断を行なう（ステップＳ５１０）。

【０１４６】

携帯電話機１００とメモリカード１１０のユーザＩＤが一致している場合は、処理はステップＳ５１４に移行し、コンテンツキーの抽出および暗号化されたコンテンツデータの出力が行なわれる。

【０１４７】

一方、携帯電話機１００とメモリカード１１０のユーザＩＤが一致しない場合（ステップＳ５１０）、コントローラ１４２０は、携帯電話機１００に対して再生不可の通知を行ない（ステップＳ５１２）、処理は終了する（ステップＳ５２０）。

【０１４８】

以上のような処理により、コンテンツデータごとに、ライセンス情報データに基づいた著作権保護ならびにユーザＩＤデータや保持情報に基づいたユーザ保護を行なった上で、コンテンツデータ（音楽データ）の再生処理を行なうことが可能となる。

【０１４９】

［消去処理］

図１２は、メモリカード１１０中に保持されたコンテンツデータの消去動作を説明するためのフローチャートである。

【０１５０】

処理が開始され、ユーザが携帯電話機１００のキータッチ部１１０８等からコンテンツデータＤｃ（ｉ）の消去指示を行なう（ステップＳ６００）。まず、メモリカード１１０のコントローラ１４２０は、メモリカード１１０に対する保守情報を記録した第１の保守情報保持部１５２０中のメディア消去フラグの値を確認する（ステップＳ６０２）。

【０１５１】

メディア消去フラグにより、消去可能が指示されている場合処理は次のステップに進み、消去禁止が指示されている場合は、コントローラ１４２０は、携帯電話機１００に対して消去不可の通知を行ない（ステップＳ６１０）、処理は終了する（ステップＳ６１２）。

【０１５２】

メディア消去フラグが消去可能を指定している場合、コントローラ１４２０は、さらに、消去が指示されたコンテンツデータＤｃ（ｉ）に対するコンテンツデータ単位の保守情報を第２の保守情報保持部１５４０に対して照会し、コンテンツ消去フラグの値を確認する（ステップＳ６０４）。

【０１５３】

当該コンテンツデータＤｃ（ｉ）の消去可能がコンテンツ消去フラグにより指定されている場合は、処理は次のステップに移行する。一方、消去禁止が指示されている場合は、コントローラ１４２０は、消去不可の通知を携帯電話機１００に対して出力し（ステップＳ６１０）、処理は終了する（ステップＳ６１２）。

【０１５４】

コンテンツ消去フラグにより当該コンテンツデータＤｃ（ｉ）の消去可能が指示されている場合は、続いて、コントローラ１４２０は、ライセンス情報保持部１５００中のコンテンツデータＤｃ（ｉ）に対応したライセンス情報データＬｉｃｅｎｓｅ（ｉ）の消去動作を行ない（ステップＳ６０６）、メモリ１４１２中

に保持された当該コンテンツデータに対応する暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）およびこれに対応する暗号化されたコンテンツキーおよび暗号化されたライセンス情報データ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）の消去動作を行なって（ステップＳ６０８）、処理が終了する（ステップＳ６１２）。

【０１５５】

以上のような処理を行なうことで、メモリカードごとに消去動作が可能か否かの指定ができるとともに、各コンテンツデータ単位で消去動作が許可されるかどうかが保守情報により指定されているので、当該コンテンツデータを配信されたユーザの許可なく、メモリ１４１２中のコンテンツデータが消去されてしまうことを防止することが可能となる。

【０１５６】

［移動処理（保守情報を考慮した場合：コンテンツデータの出力側）］

図１３は、保守情報を考慮した場合において、メモリカード１１２を移動元としてコンテンツデータの移動処理を行なう場合の処理の流れを説明するためのフローチャートであり、図８および図９で説明したカード１１２の処理と対比される図である。

【０１５７】

処理が開始されると、まず、ユーザは、携帯電話機１０２のキータッチ部１１０８等を介して、コンテンツデータＤｃ（ｉ）の移動指示を行ない（ステップＳ７００）、続いて、メモリカード１１２のコントローラ１４２０は、まず第１の保守情報保持部１５２０に登録されたメディア単位の保守情報を照会して、メディア消去フラグの値を確認する（ステップＳ７０２）。

【０１５８】

メディア消去フラグが消去可能を指示している場合は、処理は次のステップに移行し、消去禁止が指示されている場合は、メモリカード１１２のコントローラ１４２０は、携帯電話機１０２に対して移動不可の通知を行なって（ステップＳ７２０）、処理は終了する（ステップＳ７２２）。

【０１５９】

メディア消去フラグが消去可能を指示している場合は（ステップＳ７０２）、続いて、メモリカード１１２のコントローラ１４２０は、コンテンツデータＤｃ（ｉ）に対するコンテンツデータ単位の保守情報を第２の保守情報保持部１５４０に対して照会し、コンテンツ消去フラグのレベルを確認する（ステップＳ７０４）。

【０１６０】

当該コンテンツデータＤｃ（ｉ）に対する消去禁止が指示されている場合は、コントローラ１４２０は、携帯電話機１０２に対して移動不可を通知して（ステップＳ７２０）、処理は終了する（ステップＳ７２２）。

【０１６１】

一方、コンテンツ消去フラグが消去可能を指示している場合は、メモリカード１１２のコントローラ１４２０は、ＫＰｍｃ（１）保持部１４０５から、公開暗号化キーＫＰｍｃ（１）を取得し（ステップＳ７０６）、続いて、メモリ１４１２中に格納されている暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）を携帯電話機１００を介して、移動先のメモリカード１１０に対して出力する（ステップＳ７０８）。

【０１６２】

続いて、メモリカード１１２のコントローラ１４２０は、復号処理部１４１６を制御して、メモリ１４１２中に保持されたデータ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（２）を、自身の秘密復号鍵Ｋｍｃ（２）により復号する（ステップＳ７１０）。

【０１６３】

さらに、メモリカード１１２のコントローラ１４２０は、暗号化処理部１４１４を制御して、この復号されたコンテンツキーデータおよびライセンス情報データを、移動先のメモリカード１１０から送信された移動先のメモリカード１１０に対する公開暗号化キーＫＰｍｃ（１）により暗号化して、データ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）を生成して、携帯電話機１０２を介して、移動先のメモリカード１１０に対して出力する（ステップＳ７１２）。

【０１６４】

続いて、メモリカード１１２のコントローラ１４２０は、ライセンス情報保持部１５００中に保持されたコンテンツデータＤｃ（ｉ）に対応したライセンス情報データＬｉｃｅｎｓｅ（ｉ）の消去を行なう（ステップＳ７１４）。

【０１６５】

続いて、メモリカード１１２のコントローラ１４２０は、携帯電話機１０２のディスプレイ等を介して、ユーザにメモリ１４１２中のデータ消去を行なうか否かの確認を行ない、ユーザからキータッチ部１１０８等を介して消去が指示された場合は（ステップＳ７１６）、メモリ１４１２中の暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）および暗号化されたコンテンツキーおよびライセンス情報データを消去して（ステップＳ７１８）、処理が終了する（ステップＳ７２２）。

【０１６６】

一方、ユーザがメモリ１４１２中のデータ消去を指示しなかった場合は、メモリ１４１２中の暗号化されたコンテンツデータ、暗号化されたコンテンツキーデータおよびライセンス情報データを消去することなく処理が終了する（ステップＳ７２２）。

【０１６７】

コンテンツデータの一括した移動の場合と同様に、メモリ１４１２内の暗号化されたコンテンツデータの消去を行なわなかった場合も、ライセンス情報保持部１５００中の当該コンテンツデータＤｃ（ｉ）に対応したライセンス情報データは消去されているので、このままではメモリカード１１０は当該コンテンツデータの再生処理を行なうことはできない。

【０１６８】

以上のようにして、コンテンツデータ単位で保守情報を参照しつつ、移動元のメモリカード１１２から移動先のメモリカード１１０に対してコンテンツデータの移動を行なうことが可能となる。

【０１６９】

［配信・移動処理（保守情報を考慮した場合：コンテンツデータの受け側）］

図１４は、メモリカード１１０に対して、たとえば、移動動作において受信側

となっている場合、保守情報を考慮したときのコンテンツデータの追記を行なう処理を説明するためのフローチャートであり、図８および図９で説明したカード１１０の処理と対比される図である。

【０１７０】

コンテンツデータの追記としては、上述のとおり、コンテンツデータをメモリカード間で移動させる場合に受信してもよいし、あるいは、たとえば、携帯電話網を介して配信サーバ１０から配信を受ける構成としてもよいし、街頭に設置されたコンテンツデータ販売機を介して、メモリカードに直接コンテンツデータが書込まれる構成としてもよい。

【０１７１】

処理が開始されると、ユーザ２は、携帯電話機１０２のキータッチ部１１０８等を介して、コンテンツデータＤｃ（ｉ）の移動（記録）指示をメモリカード１１０に対して与える（ステップＳ８００）。

【０１７２】

続いて、メモリカード１１０のコントローラ１４２０は、メディア単位の保守情報を第１の保守情報保持部１５２０に対して照会し、追記フラグのレベルを確認する（ステップＳ８０２）。追記が禁止されている場合、コントローラ１４２０は、携帯電話機１００に対して移動不可の通知を出力し（ステップＳ８１６）、処理が終了する（ステップＳ８１８）。この移動不可の通知は、携帯電話機１００から携帯電話機１０２にさらに伝達される。

【０１７３】

一方、追記フラグにより追記可能が指示されている場合は、メモリカード１１０は、ＫＰｍｃ（１）保持部１４０５から、メモリカード１１０に対する公開暗号化キーＫＰｍｃ（１）を追記に対する移動元（メモリカード１１２）に対して出力し（ステップＳ８０４）、移動元から暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）を受けて、メモリ１４１２に格納する（ステップＳ８０６）。

【０１７４】

続いて、メモリカード１１０は、携帯電話機１００を介して、移動元からメモ

リカード１１０に対する公開暗号化キーＫＰｍｃ（１）により暗号化されたコンテンツキーデータおよびライセンス情報データ［Ｋｃ（ｉ）、Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）を受け、メモリ１４１２に対して格納する（ステップＳ８１０）。

【０１７５】

続いて、コントローラ１４２０により制御されて、復号処理部１４１６がメモリ１４１２中に保持されたコンテンツキーデータおよびライセンス情報データを秘密復号キーＫｍｃ（１）により復号し（ステップＳ８１２）、復号されたライセンス情報データＬｉｃｅｎｓｅ（ｉ）をライセンス情報保持部１５００に格納して（ステップＳ８１４）、処理が終了する（ステップＳ８１８）。

【０１７６】

以上のような処理を行なうことで、コンテンツデータ単位の追記動作を行なうことが可能となる。

【０１７７】

すなわち、第１には、メモリカードにはユーザＩＤデータＵｓｅｒ－ＩＤｍが保持され、携帯電話機には、ユーザＩＤデータＵｓｅｒ－ＩＤｈが保持される構成とすることで、メモリカードのユーザと携帯電話機のユーザとが一致しないかぎり、保守情報やユーザＩＤデータＵｓｅｒ－ＩＤｍを変更することが出来ないため、正規にコンテンツデータを購入したユーザを保護することが可能となる。

【０１７８】

しかも、第２には、再生処理、移動処理、消去処理等において、ユーザの設定した保守情報により、コンテンツデータが正規の購入者に無断で、再生されたり、消去されたり、他のメモリカードに移動されたりすることを防止することが可能となる。

【０１７９】

［実施の形態２］

実施の形態１のメモリカードでは、メモリカードのユーザと携帯電話機のユーザとが一致しないかぎり、保守情報やユーザＩＤデータＵｓｅｒ－ＩＤｍを変更することが出来ない構成とし、しかも、再生処理、移動処理、消去処理等におい

て、ユーザの設定した保守情報により、コンテンツデータが正規の購入者に無断で、再生されたり、消去されたり、他のメモリカードに移動されたりすることを防止する構成であった。

【０１８０】

実施の形態２のメモリカードでは、さらに、コンテンツデータの移動の制限として、メモリカードのユーザＩＤデータとそれが装着される携帯電話機のユーザＩＤデータの２つのユーザＩＤが一致しない場合には、コンテンツデータに対応したライセンス情報の移動または消去が禁止される。

【０１８１】

まず、実施の形態１と同様に、ユーザＩＤデータＵｓｅｒ－ＩＤｍをメモリカード１１０のユーザＩＤ保持部１５２０が記録し、携帯電話機１００においてもユーザＩＤ保持部１１０７にユーザＩＤデータＵｓｅｒ－ＩＤｈを記録しているものとする。

【０１８２】

図１５は、このような構成を有する携帯電話機１００が、メモリカード１１０を装着した状態で、配信サーバ１０および配信キャリア（携帯電話会社）２０を介して、コンテンツデータの配信を受ける状態を示す概念図である。

【０１８３】

図１５に示した構成では、ｉ番目のコンテンツデータＤｃ（ｉ）に対する再生情報Ｒｅａｄ（ｉ）として、コンテンツ復号キーＫｃ（ｉ）、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ（ｉ）およびコンテンツデータの配信を受けた際のユーザを示すユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）の組合せを用いた場合の構成を示す。

【０１８４】

ここで、このコンテンツデータごとに対応し、ライセンス情報中に含まれるユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）は、当該コンテンツデータ配信の際にユーザＩＤデータＵｓｅｒ－ＩＤｈの値が転写される。

【０１８５】

配信サーバ１０から携帯電話網を介して暗号化されたコンテンツデータＤｃ（

ｉ）が配信された場合、携帯電話機に記録されているユーザＩＤデータＵｓｅｒ－ＩＤｈは“０９０００００００００１”であり、かつ、メモリカード１１０中に保持されるユーザＩＤデータＵｓｅｒ－ＩＤｍも“０９０００００００００１”という値が保持されているものとする。このとき、コンテンツデータＤｃ（ｉ）に対応した再生情報Ｒｅａｄ（ｉ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）も“０９０００００００００１”であるものとする。

【０１８６】

再生情報Ｒｅａｄ（ｉ）は、暗号化キーＫＰｍｃ（１）により暗号化されたデータ［Ｒｅａｄ（ｉ）］Ｋｍｃ（１）として、メモリカード１１０中のメモリ１４１２に保持されているものとする。

【０１８７】

さらに、メモリカード１１０のメモリ１４１２中には暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）が保持されている。

【０１８８】

図１６は、２つのメモリカード１１０と１１２との間で、再生情報の移動が許可される場合を示す概念図である。

【０１８９】

図１６に示した場合は、送信元の携帯電話機１００では、メモリカード１１０のユーザＩＤデータＵｓｅｒ－ＩＤｍと、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈとが一致している。

【０１９０】

このような場合には、メモリカード１１０からメモリカード１１２に対して、暗号化コンテンツデータのみならず暗号化再生情報Ｒｅａｄ（ｉ）の移動が許可されて、暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）を携帯電話機１０２の側でも再生することが可能になる。メモリカード１１０のライセンス情報保持部１５００からは、実施の形態１と同様に、暗号化コンテンツデータと再生情報の双方がメモリカード１１２に移動するのに伴なって、再生情報が消去される。

【０１９１】

図１７は、２つのメモリカード１１０と１１２との間で、再生情報の移動が許可されない場合を示す概念図である。

【０１９２】

送信元の携帯電話機１００では、メモリカード１１０のユーザＩＤデータＵｓｅｒ－ＩＤｍと、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈとは一致していない。

【０１９３】

したがって、このような場合は、メモリカード１１０のコントローラ１４２０は、メモリカード１１０のメモリ１４１２中の再生情報Ｒｅａｄ（ｉ）のメモリカード１１２への転送を許可しない。

【０１９４】

このような構成とすることで、正規のユーザ以外が、無断でコンテンツデータを他のメモリカードに移動することを禁じることが可能となる。

【０１９５】

再生情報としてはコンテンツキー（暗号化コンテンツデータの復号キー）のみを含む構成としてもよいし、コンテンツキーとライセンス情報データとの組合せとしてもよい。

【０１９６】

ただし、再生情報をコンテンツキーとユーザＩＤデータとした場合、または、コンテンツ復号キー、ライセンス情報データおよびユーザＩＤデータの組合せとした場合は、以下のような処理を行なうことが可能である。

【０１９７】

すなわち、以上の説明では、携帯電話機のユーザＩＤデータとメモリカードのユーザＩＤデータとの一致／不一致に応じて、コンテンツデータに対応したライセンス情報の移動または消去が禁止される構成であった。

【０１９８】

上述のとおり、再生情報Ｒｅａｄ（ｉ）として、言いかえると、コンテンツデータごとに、ユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）がライセンス情報保持部１５００およびメモリ１４１２に格納されている場合は、このユーザＩＤデータＵ

ｓｅｒ－ＩＤ（ｉ）の値と、メモリカードのユーザＩＤデータＵｓｅｒ－ＩＤｍの値、携帯電話機のユーザＩＤデータＵｓｅｒ－ＩＤｈの値とに応じて、再生情報の移動を許可するか否かを、コンテンツデータごとに判断して、処理することが可能である。

【０１９９】

すなわち、メモリカードに記録された再生情報に含まれるユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）と、メモリカードのユーザＩＤデータＵｓｅｒ－ＩＤｍと携帯電話機に記憶されたユーザＩＤデータＵｓｅｒ－ＩＤｈとの関係から、コンテンツデータのライセンス情報の移動または消去が禁止されるという制御を行なうことが可能である。

【０２００】

図１８は、このようにコンテンツデータ単位で、再生情報の転送を制御する場合の構成を示す概念図である。

【０２０１】

なお、実施の形態１の図１０で説明したのと同様に、携帯電話機のユーザＩＤデータＵｓｅｒ－ＩＤｈとメモリカードのユーザＩＤデータＵｓｅｒ－ＩＤｍと、コンテンツデータＤｃ（ｉ）に対応したユーザ情報データ中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）とが一致している場合にユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）を書きかえることで、ユーザＩＤに対する制限を解除することが可能である。また、コンテンツデータＤｃ（ｉ）に対応したユーザ情報データ中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）が記憶されていない場合は、ユーザＩＤに対する制限は、働かないものとする。

【０２０２】

以上のような構成とした場合、メモリカード１１０からメモリカード１１２へ再生情報の移動が行なわれた後の状態としては、たとえば、以下の５通りのような場合がある。

【０２０３】

まず、図１８においても、図１５と同様に、ｉ番目のコンテンツデータＤｃ（ｉ）に対する再生情報Ｒｅａｄ（ｉ）として、コンテンツ復号キーＫｃ（ｉ）、

ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ（ｉ）およびコンテンツデータの配信を受けた際のユーザを示すユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）の組合せを用いる。

【０２０４】

また、携帯電話機１００に記録されているユーザＩＤデータＵｓｅｒ－ＩＤｈは“０９０００００００１”であり、かつ、メモリカード１１０中に保持されるユーザＩＤデータＵｓｅｒ－ＩＤｍも“０９０００００００１”という値が保持されているものとする。携帯電話機１０２に記録されているユーザＩＤデータＵｓｅｒ－ＩＤｈは“０９０００００００２”であり、かつ、メモリカード１１２中に保持されるユーザＩＤデータＵｓｅｒ－ＩＤｍも“０９０００００００２”という値が保持されているものとする。

【０２０５】

さらに、再生情報Ｒｅａｄ（ｉ）は、暗号化キーＫＰｍｃ（１）により暗号化されたデータ［Ｒｅａｄ（ｉ）］Ｋｍｃ（１）として、メモリカード１１０中のメモリ１４１２に保持されているものとする。

【０２０６】

図１８を参照して、まず、第１の場合としては、メモリカード１１０において、コンテンツデータＤｃ（ｉ）に対応した再生情報Ｒｅａｄ（ｉ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）も“０９０００００００１”であるものとする。この場合、メモリカード１１０のユーザＩＤデータＵｓｅｒ－ＩＤｍと携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈが一致し、かつ、コンテンツデータＫｃ（ｉ）に対応したユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）もこれらと一致するので、再生情報の移動が許可され、かつ、メモリカード１１２に移動後も、再生情報Ｒｅａｄ（ｊ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｊ）は“０９０００００００１”のままである。

【０２０７】

第２の場合としては、上記第１の場合の移動後に、携帯電話機１０２において、再生情報Ｒｅａｄ（ｊ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｊ）を“０９０００００００２”にした場合である。

【０２０８】

第３の場合としては、上記第１の場合の移動後に、携帯電話機１０２において、再生情報Ｒｅａｄ（ｊ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｊ）を消去した場合である。

【０２０９】

第４の場合としては、もともと、再生情報Ｒｅａｄ（ｉ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）は記録されていない場合である。この場合は、再生情報の移動が許可され、ユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）による移動の制限はない。

【０２１０】

第５の場合は、第４の場合において、さらにユーザが携帯電話機１０２の側で、再生情報Ｒｅａｄ（ｊ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｊ）を“０９０００００００２”とした場合である。

【０２１１】

以上、第１から第５のいずれの場合も、メモリカード１１０のライセンス情報保持部１５００からは、暗号化コンテンツデータと再生情報の双方がメモリカード１１２に移動するのに伴なって、再生情報が消去される。

【０２１２】

図１９は、これらに対して、このようにコンテンツデータ単位で、再生情報の転送を制御した場合に、ライセンス情報の移動が禁止されるときを示す概念図である。

【０２１３】

移動元の携帯電話機１００においては、メモリカード１１０のユーザＩＤデータＵｓｅｒ－ＩＤｍと、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈとは一致しているものの、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈと再生情報Ｒｅａｄ（ｉ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）とが一致しないため、再生情報の移動が禁止される。

【０２１４】

このような構成により、メモリカードという携帯電話機から着脱可能な記録媒

動、複製においてはコンテンツデータとともに処理され、再生時には分離されて音楽データとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ１４１２に記録される。

【０２２０】

なお、以上の説明では、メモリカードとしての構成を説明したが、本発明はこのような構成に限定されることなく、より一般に、配信された暗号化コンテンツデータを再生出力する再生装置、たとえば、携帯電話機に対して着脱可能であって、かつ、暗号化コンテンツデータの配信のために必要なキーデータ等の授受を行う機能を有して、この暗号化コンテンツデータを受けて記録する装置に対して適用可能なものである。

【０２２１】

さらに、本発明において、ユーザが音楽データなどのコンテンツデータを入手する経路としては、上述のとおり、携帯電話網や他の情報通信網を介したデータ配信に限られるものではなく、たとえば、多数のコンテンツデータを蓄えて街頭に設置されたコンテンツデータ販売機などにより販売される情報を記録する記録装置にも適用可能なものである。

【０２２２】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０２２３】

【発明の効果】

以上説明したとおり、本願発明にかかる配信システムでは、正規のユーザが受信してメモリ中に格納したコンテンツデータに対して、正規ユーザのみが再生、消去、移動処理を行なうすることが可能な構成となっているので、正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

【図面の簡単な説明】

【図１】　情報の配信を受けるための端末である携帯電話機１００の構成を説明するための概略ブロック図である。

【図２】　図１に示したメモリカード１１０の構成を説明するための概略ブロック図である。

【図３】　本発明の記録媒体が用いられる情報配信システムの全体構成を概略的に説明するための概念図である。

【図４】　図３に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図５】　図３に示した音楽サーバ３０の構成を示す概略ブロック図である。

【図６】　実施の形態１の情報配信システムにおけるコンテンツデータの配信動作を説明するためのフローチャートである。

【図７】　メモリカード１１０に保持された暗号化コンテンツデータから、音楽情報を再生処理を説明するためのフローチャートである

【図８】　２つのメモリカード間において、コンテンツデータおよびキーデータとの移動を行なう処理を説明するための第１のフローチャートである。

【図９】　２つのメモリカード間において、コンテンツデータおよびキーデータとの移動を行なう処理を説明するための第２のフローチャートである。

【図１０】　本発明のメモリカード１１０の保守情報またはユーザＩＤデータＵｓｅｒ－ＩＤｍの変更指示の処理を説明するためのフローチャートである。

【図１１】　保守情報の考慮のある場合について、メモリカード１１０のコンテンツデータＤｃ（ｉ）の再生動作を説明するためのフローチャートである。

【図１２】　メモリカード１１０中に保持されたコンテンツデータの消去動作を説明するためのフローチャートである。

【図１３】　保守情報を考慮した場合において、移動処理を行なう場合の処理の流れを説明するためのフローチャートである。

【図１４】　移動動作において受信側となっている場合、保守情報を考慮したときの追記処理を説明するためのフローチャートである。

【図１５】　メモリカード１１０がコンテンツデータの配信を受ける状態を

示す概念図である。

【図１６】　２つのメモリカード１１０と１１２との間で、再生情報の移動が許可される場合を示す概念図である。

【図１７】　２つのメモリカード１１０と１１２との間で、再生情報の移動が許可されない場合を示す概念図である。

【図１８】　コンテンツデータ単位で、再生情報の転送を制御する場合の構成を示す概念図である。

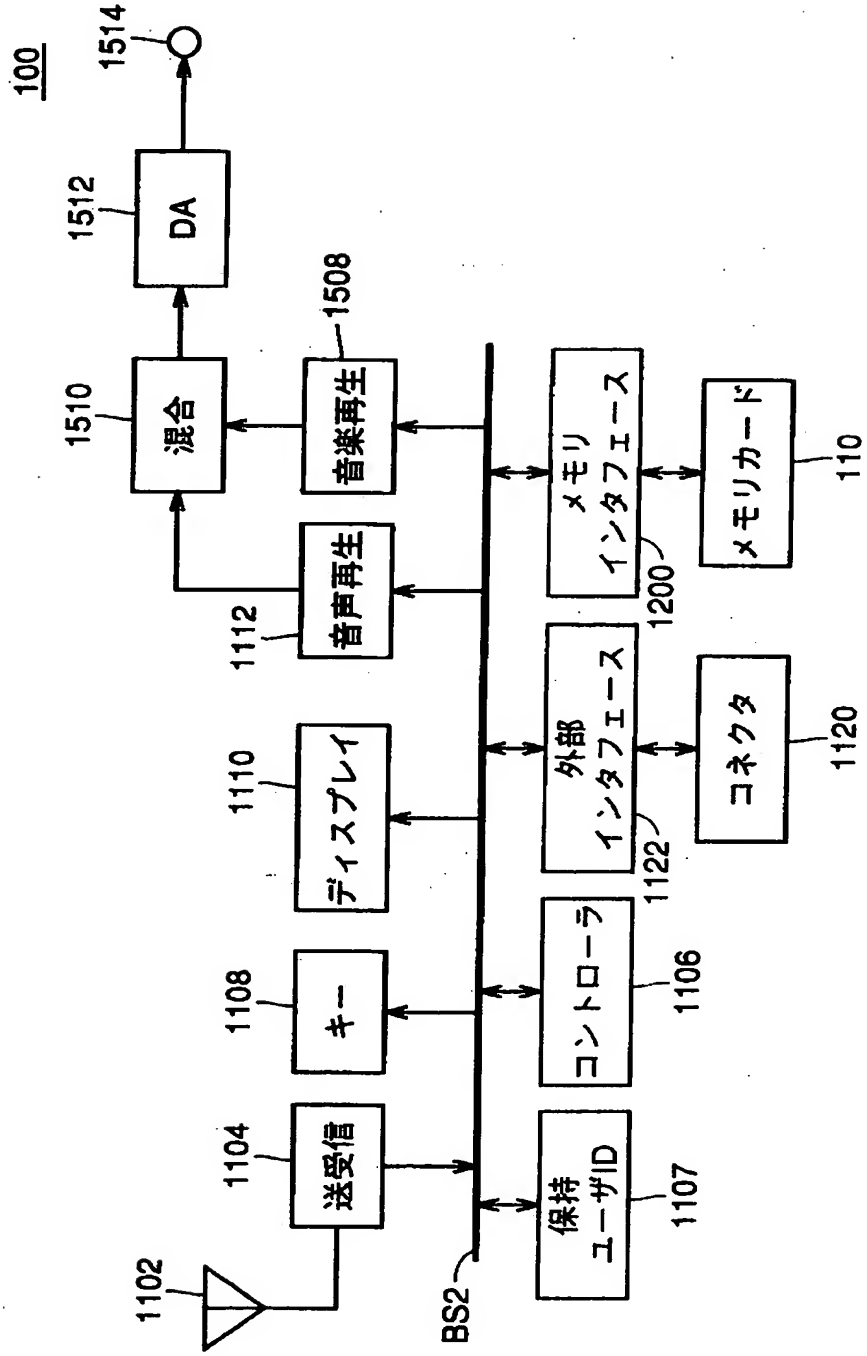
【図１９】　コンテンツデータ単位で、再生情報の転送を制御した場合に、ライセンス情報の移動が禁止されるときを示す概念図である。

【符号の説明】

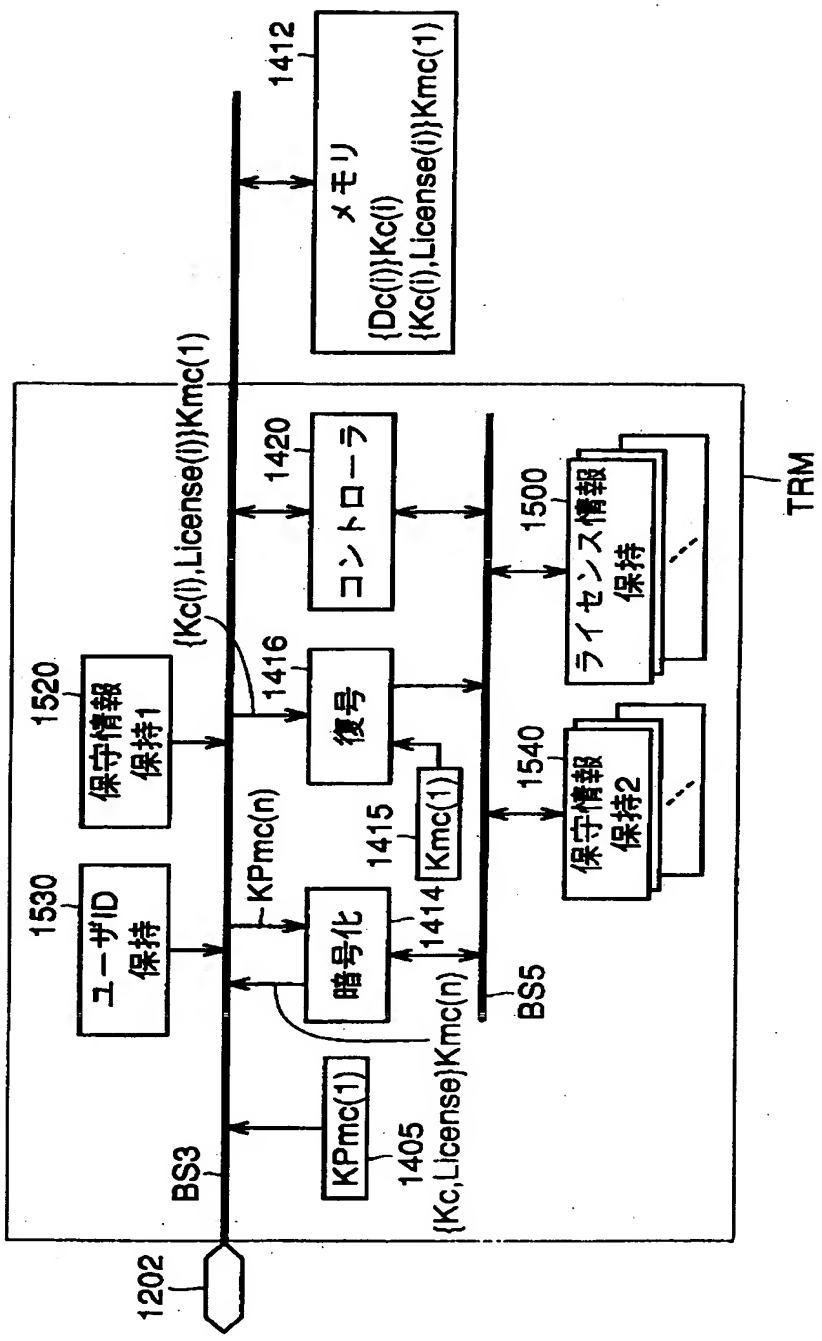
１０　配信サーバ、２０　配信キャリア、３０　音楽サーバ、１００，１０１，１０２，１０３　携帯電話機、１１０，１１２，１２０，１２２　メモリカード、１３０，１３２　ヘッドホン、１１０２　アンテナ、１１０４　送受信機、１１０６　コントローラ、１１０７　ユーザＩＤ保持部、１１０８　タッチキー部、１１１０　ディスプレイ、１１１２　音声再生部、１２００　メモリインタフェース、１４０４　復号処理部、１４０６　暗号化処理部、１４０８，１４０９　切替スイッチ、１４１０　復号処理部、１４１２　メモリ、１４１４　暗号化処理部、１４１６　復号処理部、１４２０　コントローラ、１４３０　暗号化処理部、１４３２　セッションキー発生部、１４３４，１４３５　切替スイッチ、１５００　ライセンス情報保持部、１５０２　セッションキー発生部、１５０４　暗号化処理部、１５０６　復号処理部、１５０８　音楽再生部、１５１０　混合部、１５１２　デジタルアナログ変換器、１５２０　第１の保守情報保持部、１５３０　ユーザＩＤ保持部、１５４０　第２の保守情報保持部。

【書類名】　　図面

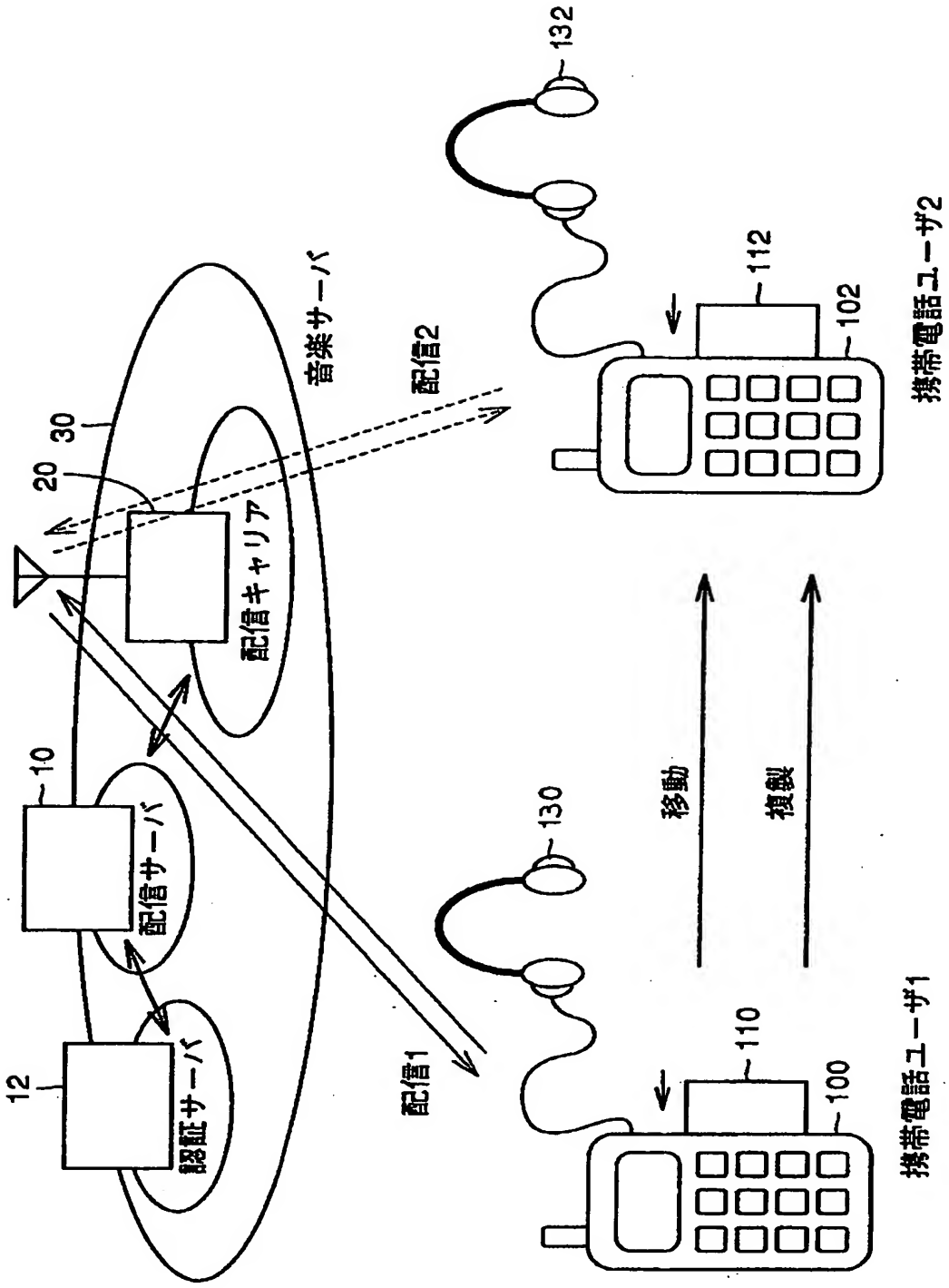
【図１】


100
1514
DA
1512
混合
1510
音楽再生
1508
音声再生
1112
ディスプレイ
1110
キー
1108
送受信
1104
1102
BS2
保持
ユーザID
1107
コントローラ
1106
外部
インタフェース
1122
メモリ
インタフェース
1200
メモリカード
110
コネクタ
1120

【図２】


110
1412
メモリ
{Dc(i)}Kc(i)
{Kc(i),License(i)}Kmc(1)
1420
コントローラ
1500
ライセンス情報保持
TRM
{Kc(i),License(i)}Kmc(1)
1520
保守情報保持1
1416
復号
1540
保守情報保持2
KPmc(n)
1415
Kmc(1)
1530
ユーザID保持
1414
暗号化
BS5
{Kc,License}Kmc(n)
KPmc(1)
1405
BS3
1202

【図３】


132
112
102
携帯電話ユーザ2
音楽サーバ
配信2
30
20
配信キャリア
10
配信サーバ
12
認証サーバ
配信1
130
移動
複製
110
100
携帯電話ユーザ1

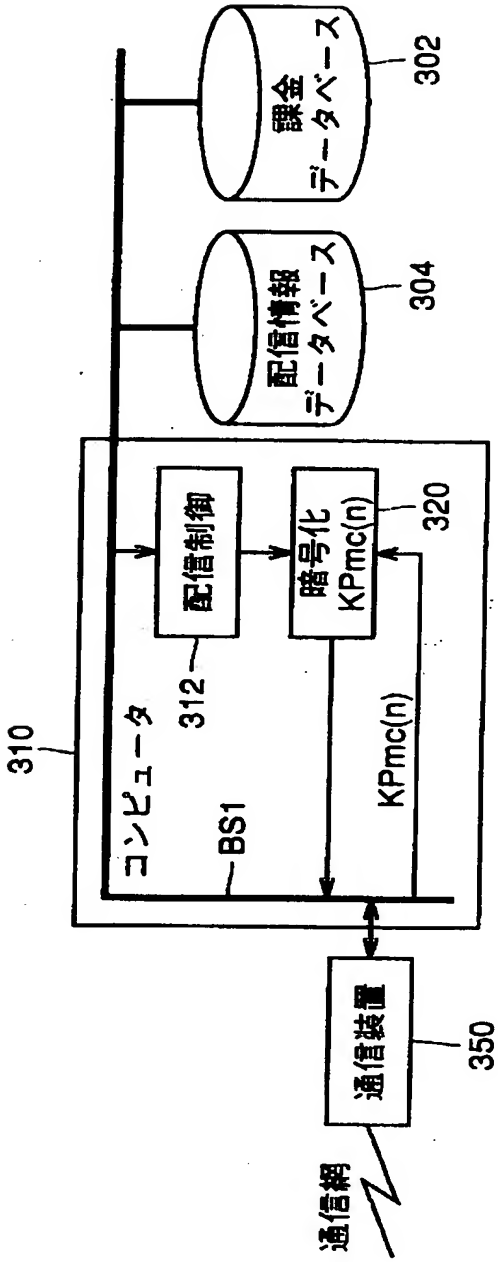
【図４】

	記号	属性	特性	
メモリカード内管理の鍵	Kmc(n)	秘密復号鍵		メモリカード毎に異なる
	KPmc(n)	公開暗号化鍵		Kmc(n)と対を成す。 KPmc(n)により暗号化されたデータは、Kmc(n)で復号可能
	User-IDm	メモリカードのユーザを識別する情報		例：ユーザの設定
メモリカード外管理の鍵	User-IDh	携帯電話機ユーザを識別する情報		例：電話番号
配信データ	Kc(i)	共通鍵	ライセンスキー	暗号化コンテンツデータの復号鍵
	License(i)	再生に関する情報	コンテンツデータごと	例：曲目の特定情報 再生回数の制限情報
	Dc(i)	コンテンツデータ		例：音楽情報データ
	[Dc]Kc	暗号化コンテンツデータ		共通鍵Kcにより暗号化されたコンテンツデータ

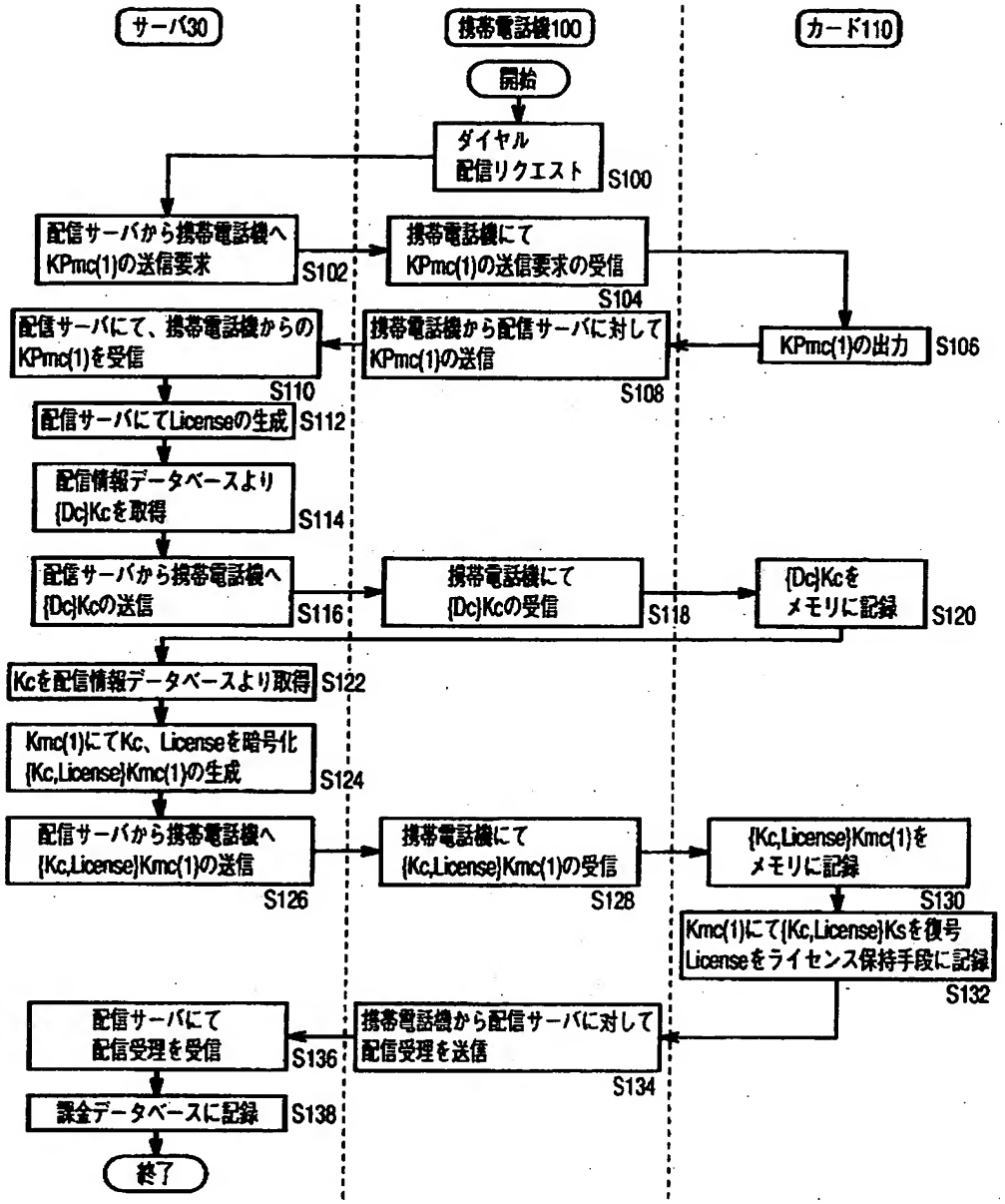
特平１１－２４３７４

出証特２０００－３０８５３２２

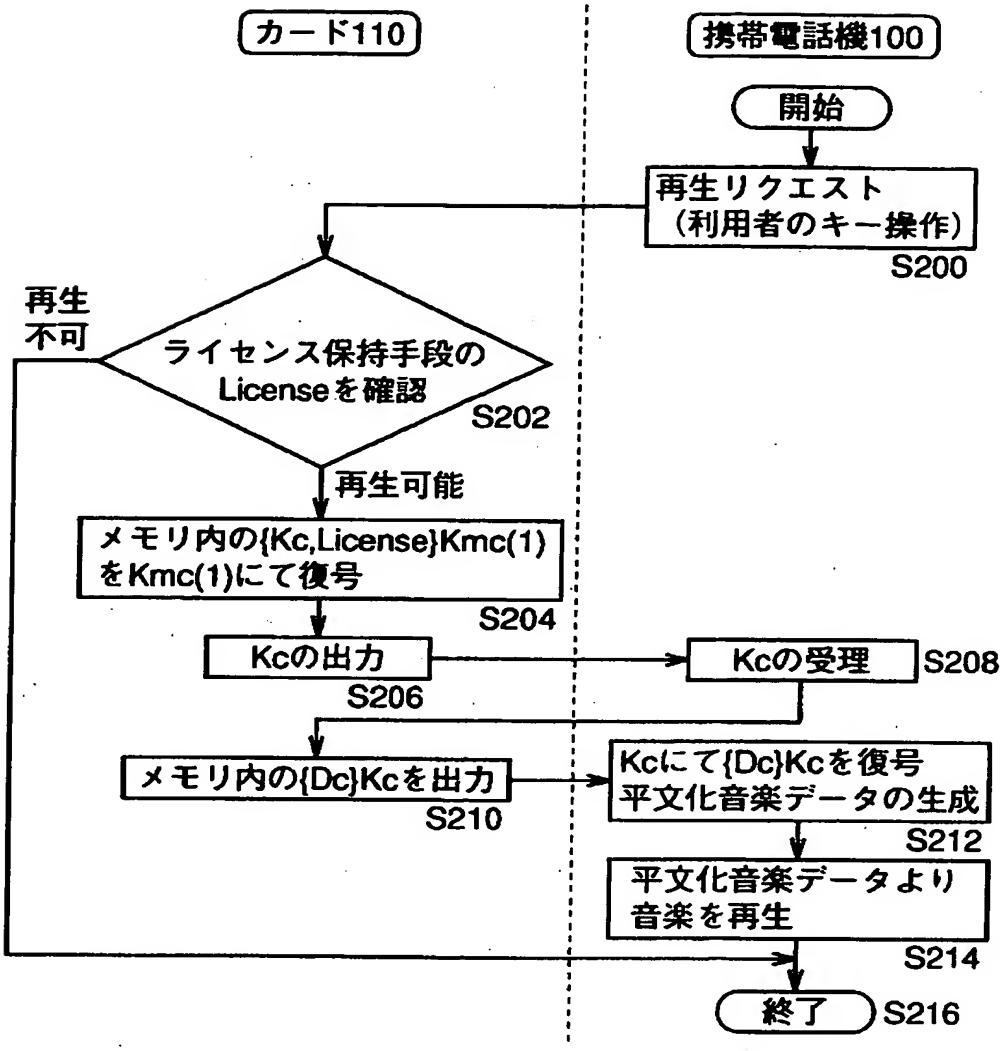
【図５】


課金
データベース
302
配信情報
データベース
304
配信制御
暗号化
KPmc(n)
320
312
310
コンピュータ
BS1
KPmc(n)
通信装置
350
通信網

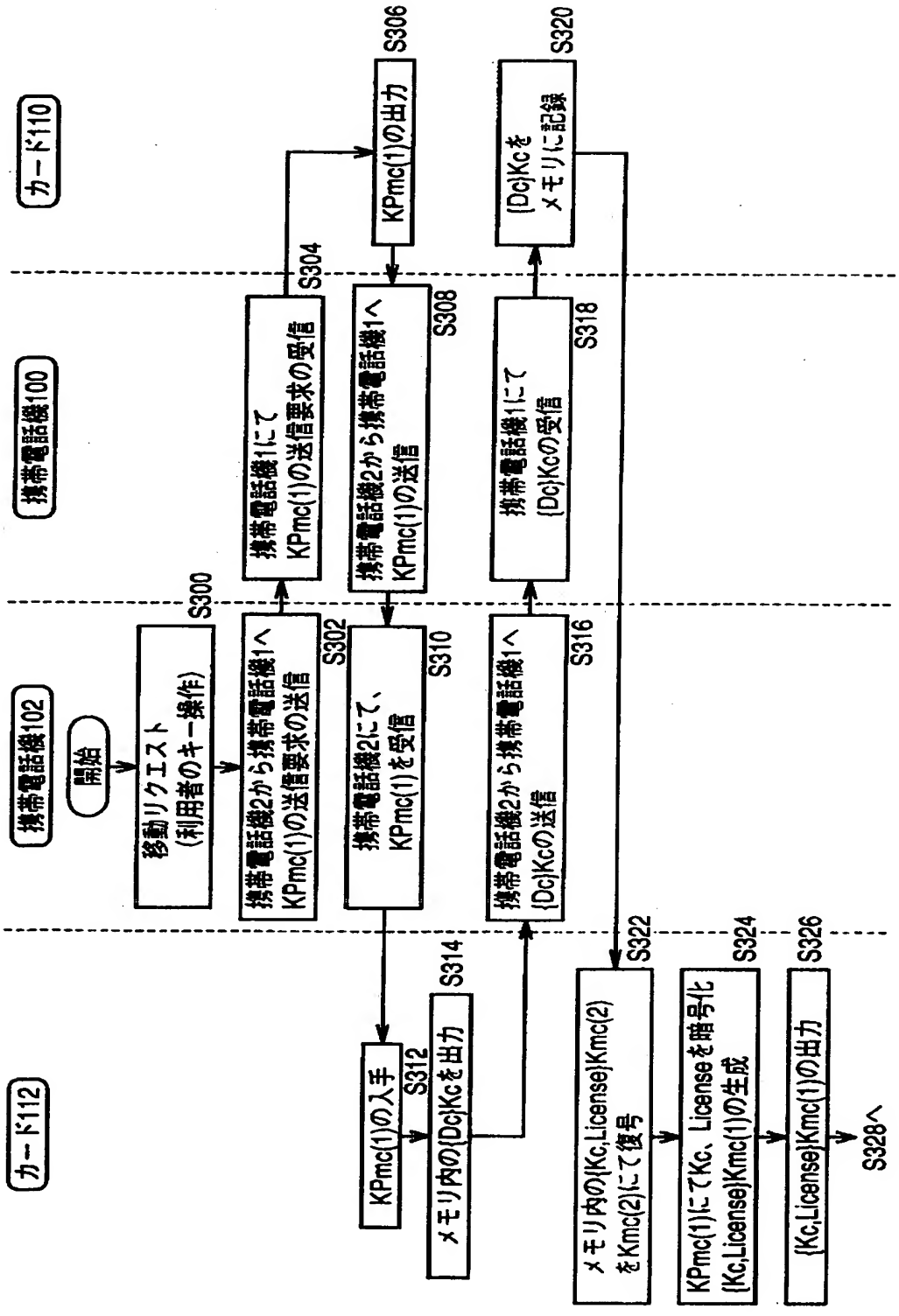
【図６】


サーバ30
携帯電話機100
カード110
開始
ダイヤル
配信リクエスト
S100
配信サーバから携帯電話機へ
KPmc(1)の送信要求
S102
携帯電話機にて
KPmc(1)の送信要求の受信
S104
KPmc(1)の出力
S106
携帯電話機から配信サーバに対して
KPmc(1)の送信
S108
配信サーバにて、携帯電話機からの
KPmc(1)を受信
S110
配信サーバにてLicenseの生成
S112
配信情報データベースより
{Dc}Kcを取得
S114
配信サーバから携帯電話機へ
{Dc}Kcの送信
S116
携帯電話機にて
{Dc}Kcの受信
S118
{Dc}Kcを
メモリに記録
S120
Kcを配信情報データベースより取得
S122
Kmc(1)にてKc、Licenseを暗号化
{Kc,License}Kmc(1)の生成
S124
配信サーバから携帯電話機へ
{Kc,License}Kmc(1)の送信
S126
携帯電話機にて
{Kc,License}Kmc(1)の受信
S128
{Kc,License}Kmc(1)を
メモリに記録
S130
Kmc(1)にて{Kc,License}Ksを復号
Licenseをライセンス保持手段に記録
S132
携帯電話機から配信サーバに対して
配信受理を送信
S134
配信サーバにて
配信受理を受信
S136
課金データベースに記録
S138
終了

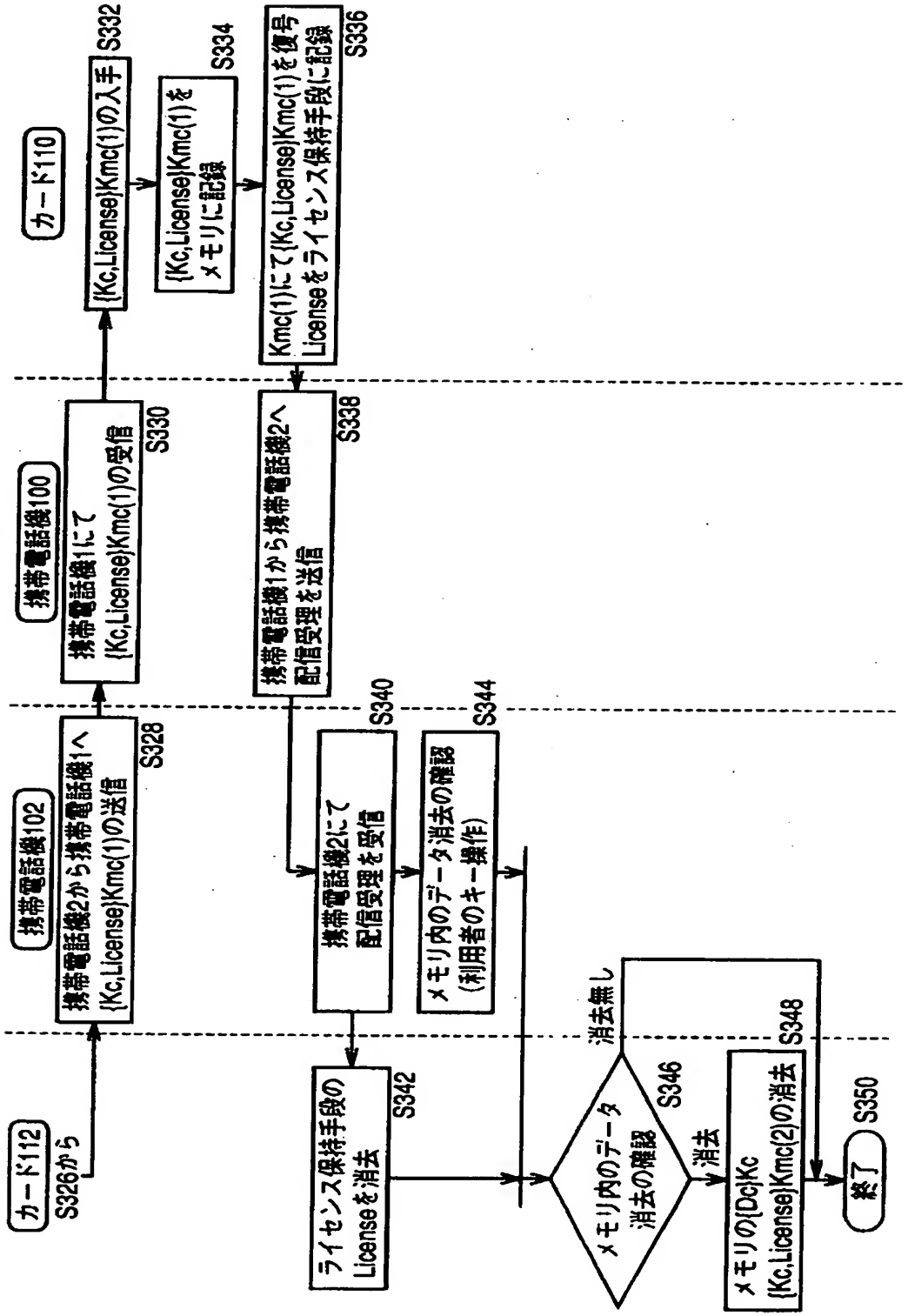
【図７】


カード110
携帯電話機100
開始
再生リクエスト
（利用者のキー操作）
S200
再生
不可
ライセンス保持手段の
Licenseを確認
S202
再生可能
メモリ内の{Kc,License}Kmc(1)
をKmc(1)にて復号
S204
Kcの出力
S206
Kcの受理
S208
メモリ内の{Dc}Kcを出力
S210
Kcにて{Dc}Kcを復号
平文化音楽データの生成
S212
平文化音楽データより
音楽を再生
S214
終了
S216

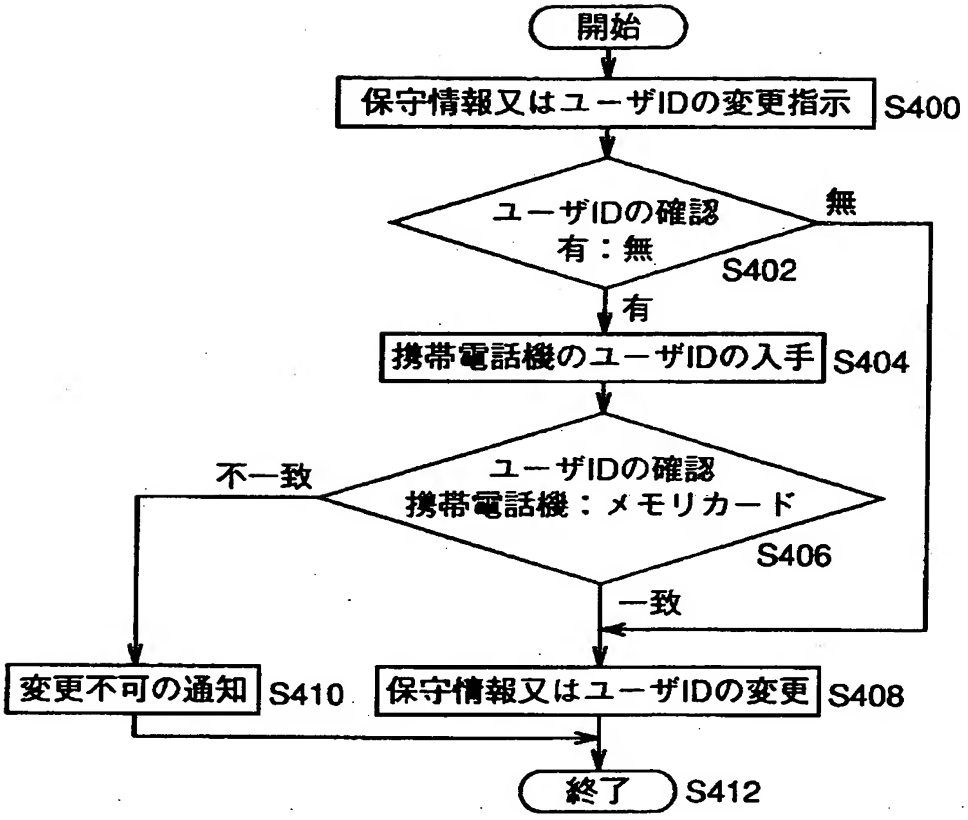
【図８】


カード110
携帯電話機100
携帯電話機102
カード112
開始
移動リクエスト
(利用者のキー操作)
S300
携帯電話機2から携帯電話機1へ
KPmc(1)の送信要求の送信
S302
携帯電話機1にて
KPmc(1)の送信要求の受信
S304
KPmc(1)の出力
S306
携帯電話機2から携帯電話機1へ
KPmc(1)の送信
S308
携帯電話機2にて、
KPmc(1)を受信
S310
KPmc(1)の入手
S312
メモリ内の{Dc}Kcを出力
S314
携帯電話機2から携帯電話機1へ
{Dc}Kcの送信
S316
携帯電話機1にて
{Dc}Kcの受信
S318
{Dc}Kcを
メモリに記録
S320
メモリ内の{Kc,License}Kmc(2)
をKmc(2)にて復号
S322
KPmc(1)にてKc、Licenseを暗号化
{Kc,License}Kmc(1)の生成
S324
{Kc,License}Kmc(1)の出力
S326
S328へ

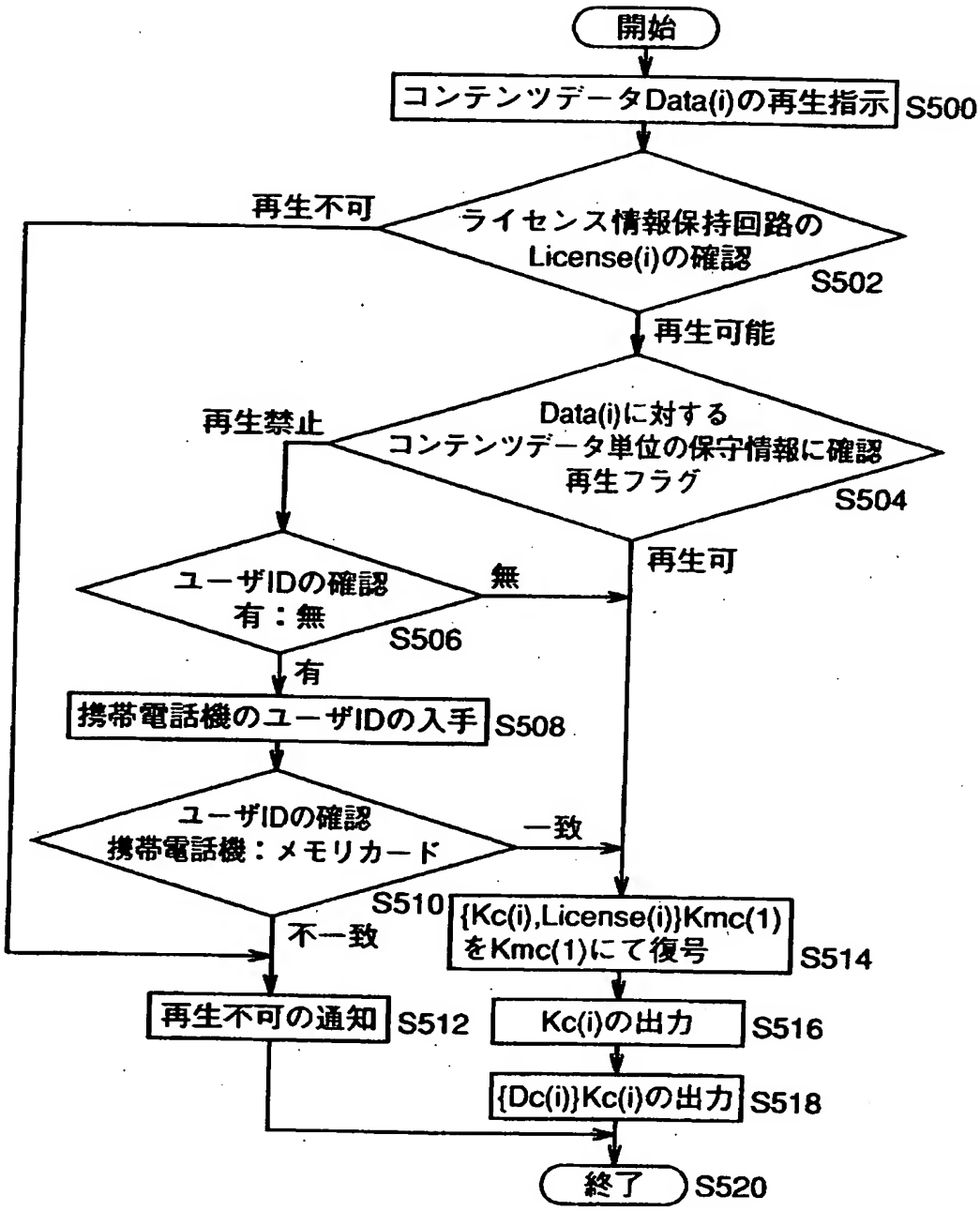
【図９】


カード112
S326から
携帯電話機102
携帯電話機2から携帯電話機1へ
{Kc,License}Kmc(1)の送信
S328
携帯電話機100
携帯電話機1にて
{Kc,License}Kmc(1)の受信
S330
カード110
{Kc,License}Kmc(1)の入手
S332
{Kc,License}Kmc(1)を
メモリに記録
S334
Kmc(1)にて{Kc,License}Kmc(1)を復号
Licenseをライセンス保持手段に記録
S336
携帯電話機1から携帯電話機2へ
配信受理を送信
S338
携帯電話機2にて
配信受理を受信
S340
メモリ内のデータ消去の確認
(利用者のキー操作)
S344
ライセンス保持手段の
Licenseを消去
S342
メモリ内のデータ
消去の確認
S346
消去無し
消去
メモリの{Dc}Kc
{Kc,License}Kmc(2)の消去
S348
終了
S350

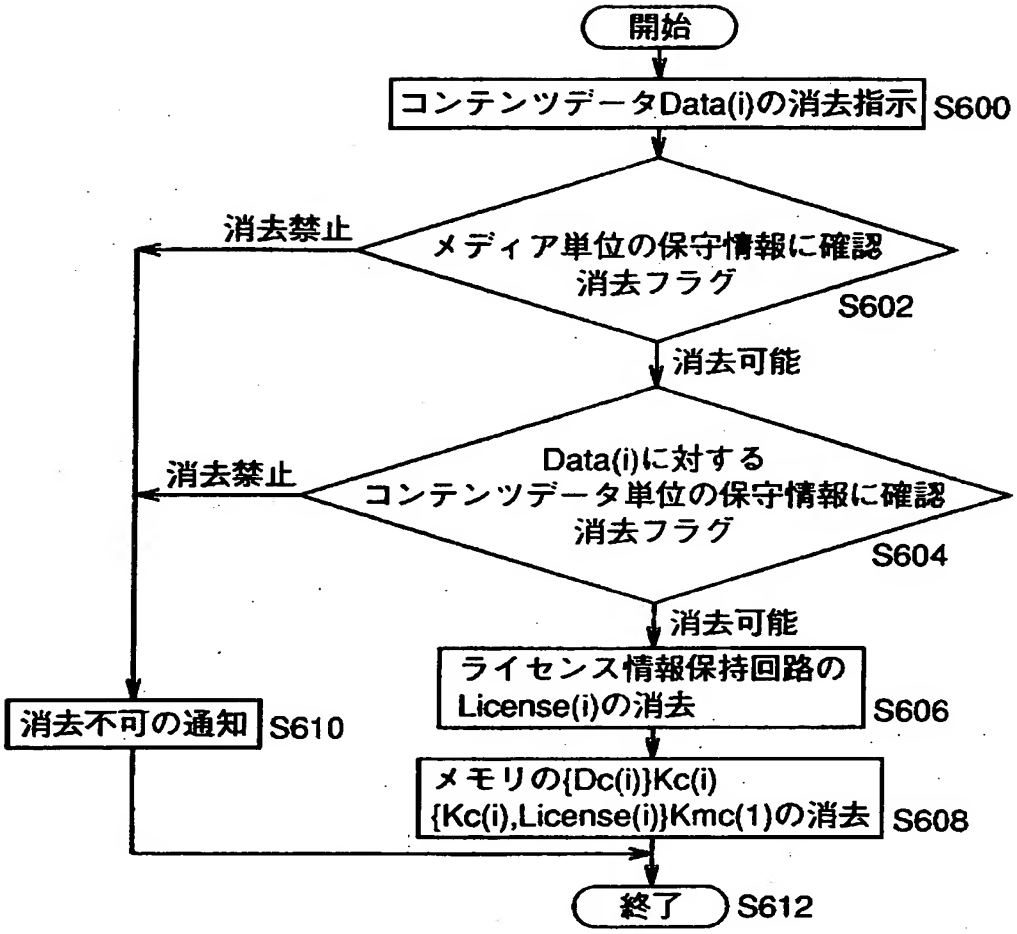
【図１０】


開始
保守情報又はユーザIDの変更指示
S400
ユーザIDの確認
有：無
S402
無
有
携帯電話機のユーザIDの入手
S404
ユーザIDの確認
携帯電話機：メモリカード
S406
不一致
一致
変更不可の通知
S410
保守情報又はユーザIDの変更
S408
終了
S412

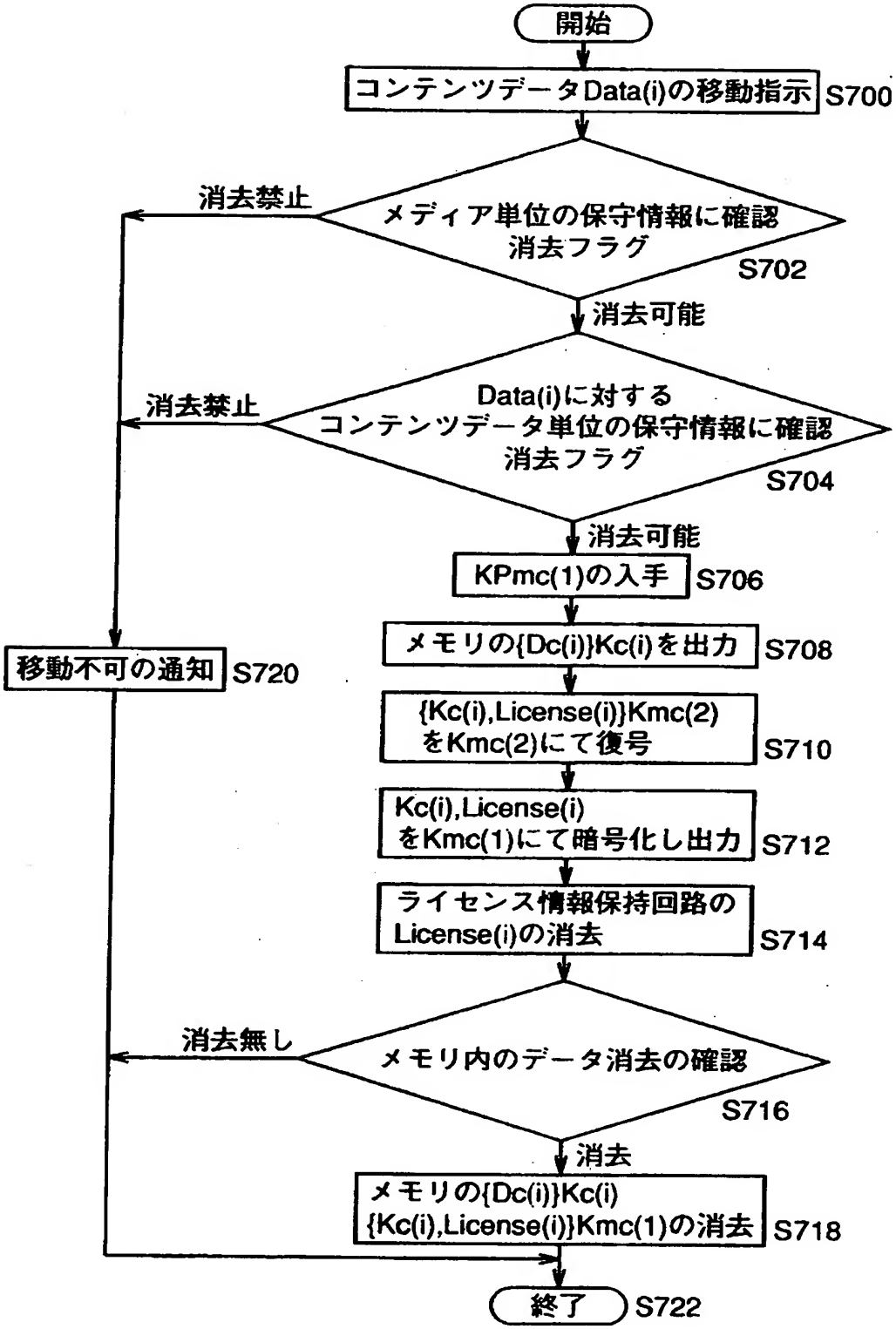
【図１１】


開始
コンテンツデータData(i)の再生指示
S500
ライセンス情報保持回路の
License(i)の確認
S502
再生不可
再生可能
Data(i)に対する
コンテンツデータ単位の保守情報に確認
再生フラグ
S504
再生禁止
再生可
ユーザIDの確認
有：無
S506
無
有
携帯電話機のユーザIDの入手
S508
ユーザIDの確認
携帯電話機：メモリカード
S510
一致
不一致
{Kc(i),License(i)}Kmc(1)
をKmc(1)にて復号
S514
再生不可の通知
S512
Kc(i)の出力
S516
{Dc(i)}Kc(i)の出力
S518
終了
S520

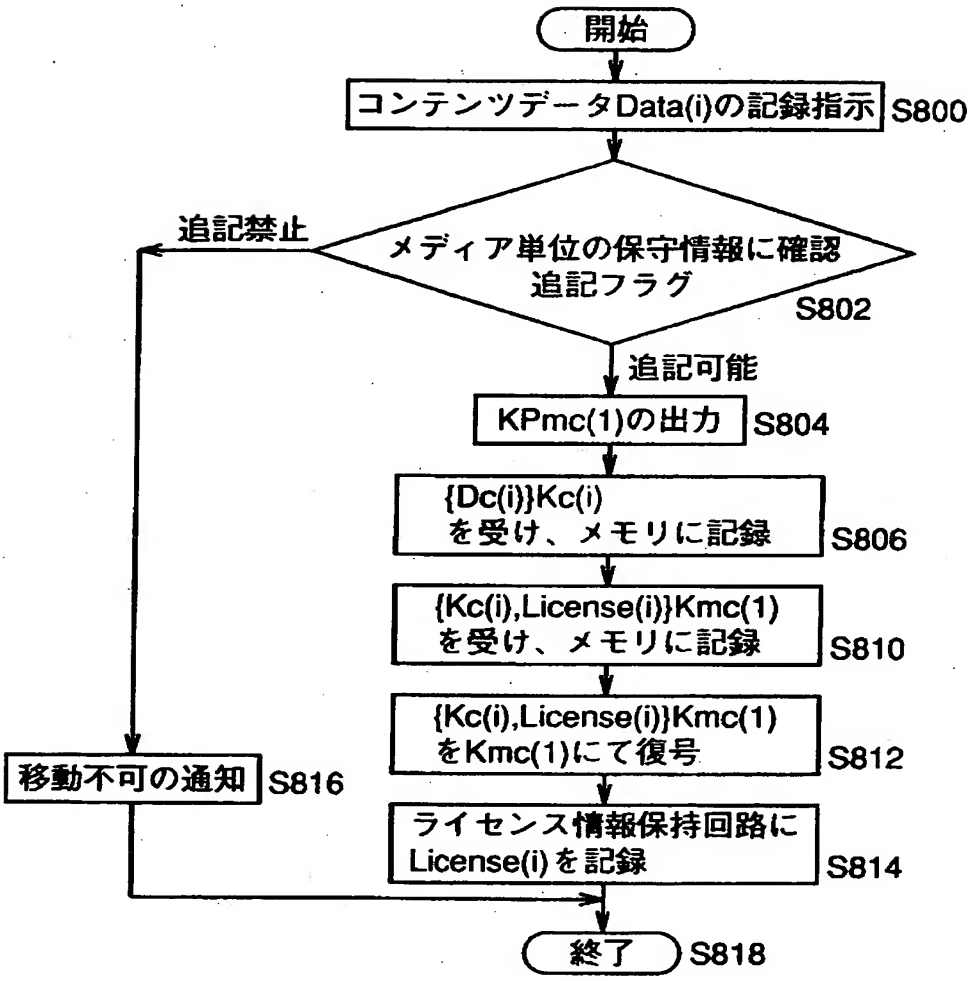
【図１２】


開始
コンテンツデータData(i)の消去指示
S600
メディア単位の保守情報に確認
消去フラグ
S602
消去禁止
消去可能
Data(i)に対する
コンテンツデータ単位の保守情報に確認
消去フラグ
S604
消去禁止
消去可能
ライセンス情報保持回路の
License(i)の消去
S606
メモリの{Dc(i)}Kc(i)
{Kc(i),License(i)}Kmc(1)の消去
S608
消去不可の通知
S610
終了
S612

【図１３】

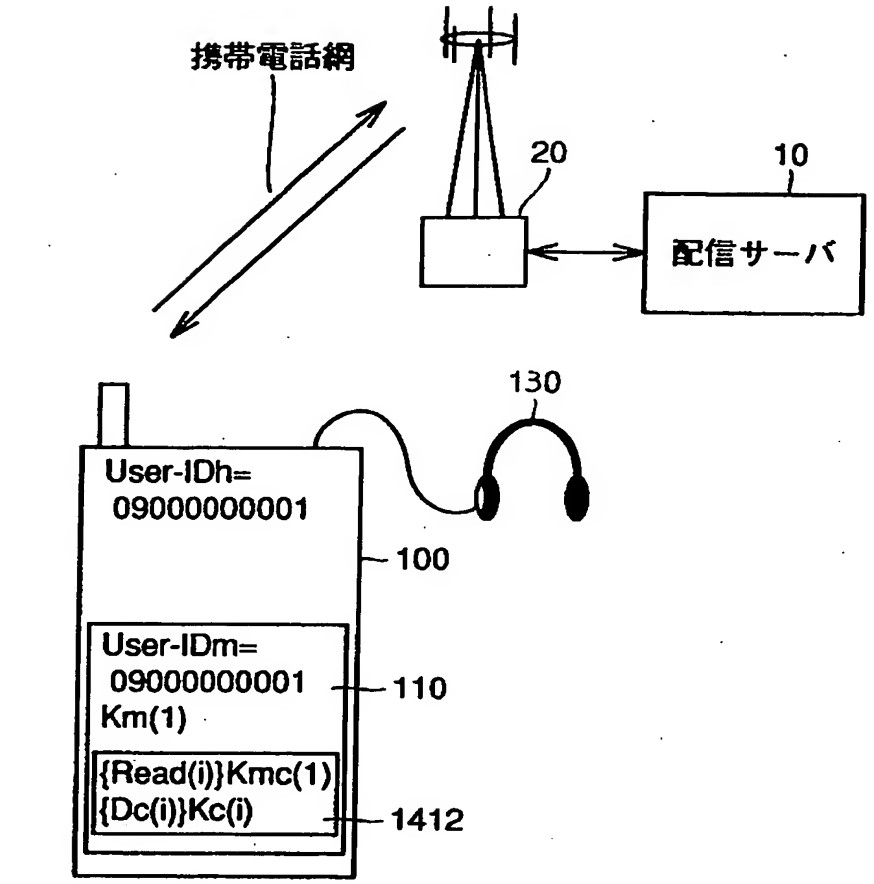

開始
コンテンツデータData(i)の移動指示
S700
メディア単位の保守情報に確認
消去フラグ
S702
消去禁止
消去可能
Data(i)に対する
コンテンツデータ単位の保守情報に確認
消去フラグ
S704
消去禁止
消去可能
KPmc(1)の入手
S706
メモリの{Dc(i)}Kc(i)を出力
S708
{Kc(i),License(i)}Kmc(2)
をKmc(2)にて復号
S710
Kc(i),License(i)
をKmc(1)にて暗号化し出力
S712
ライセンス情報保持回路の
License(i)の消去
S714
移動不可の通知
S720
メモリ内のデータ消去の確認
S716
消去無し
消去
メモリの{Dc(i)}Kc(i)
{Kc(i),License(i)}Kmc(1)の消去
S718
終了
S722

【図１４】

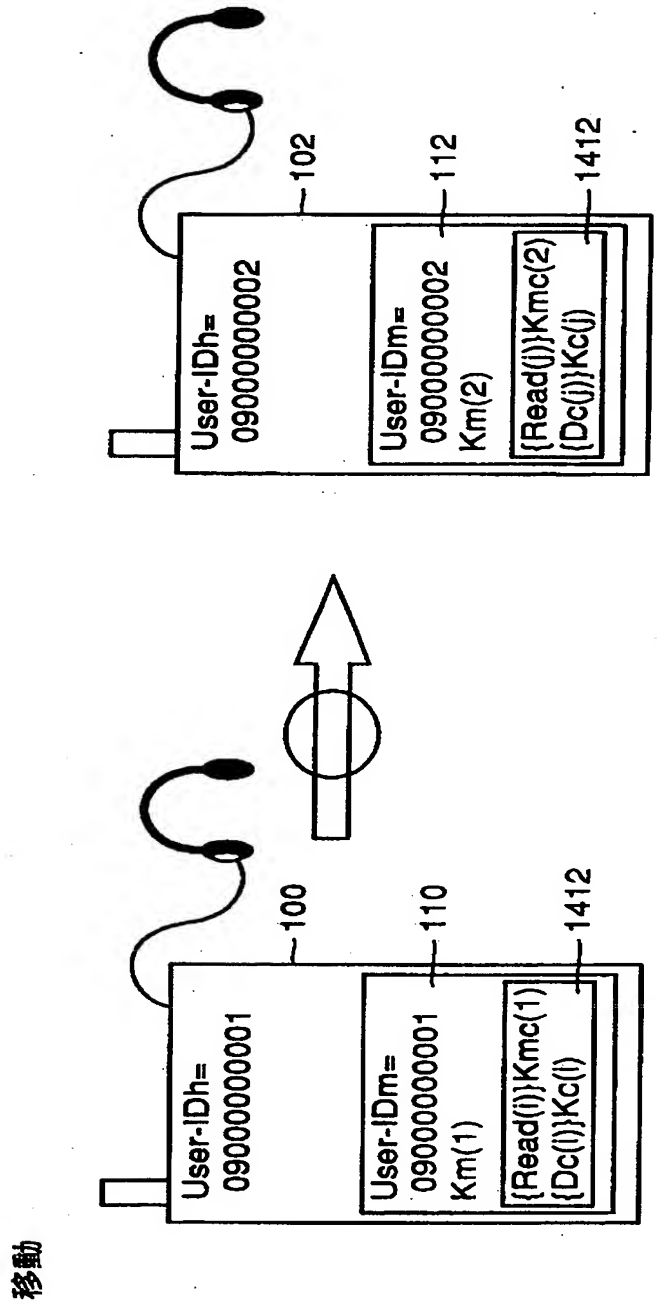

開始
コンテンツデータData(i)の記録指示
S800
メディア単位の保守情報に確認
追記フラグ
S802
追記禁止
追記可能
KPmc(1)の出力
S804
{Dc(i)}Kc(i)
を受け、メモリに記録
S806
{Kc(i),License(i)}Kmc(1)
を受け、メモリに記録
S810
{Kc(i),License(i)}Kmc(1)
をKmc(1)にて復号
S812
ライセンス情報保持回路に
License(i)を記録
S814
移動不可の通知
S816
終了
S818

【図１５】

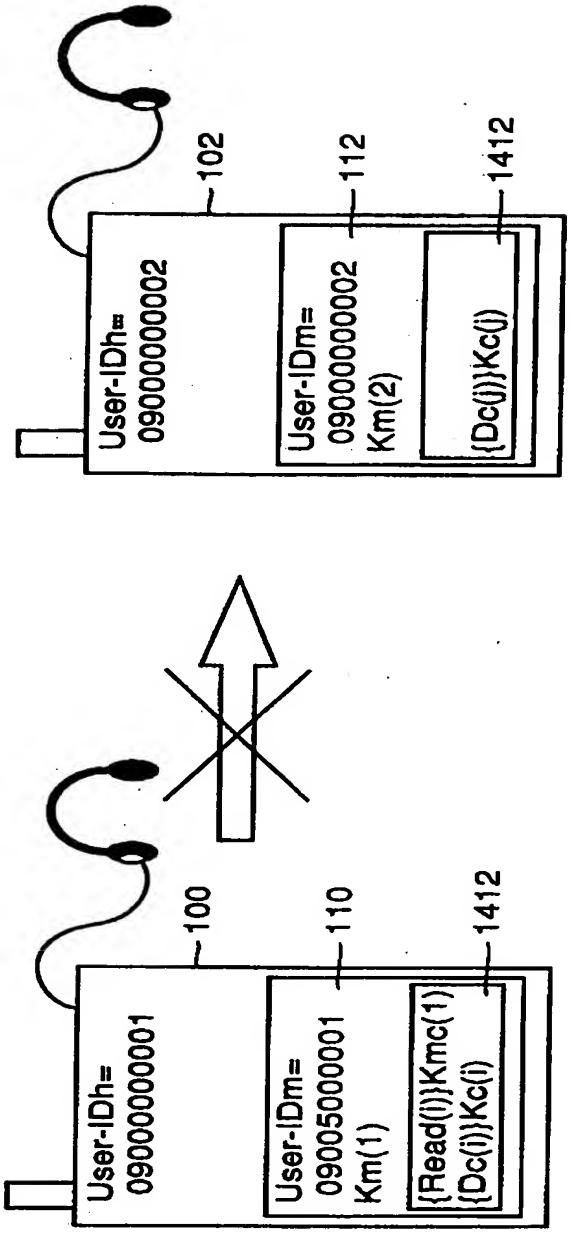
配信


携帯電話網
20
10
配信サーバ
130
User-IDh=
09000000001
100
User-IDm=
09000000001
Km(1)
110
{Read(i)}Kmc(1)
{Dc(i)}Kc(i)
1412
Read(i)=Kc(i),License(i),User-ID(i)
User-ID(i)=09000000001

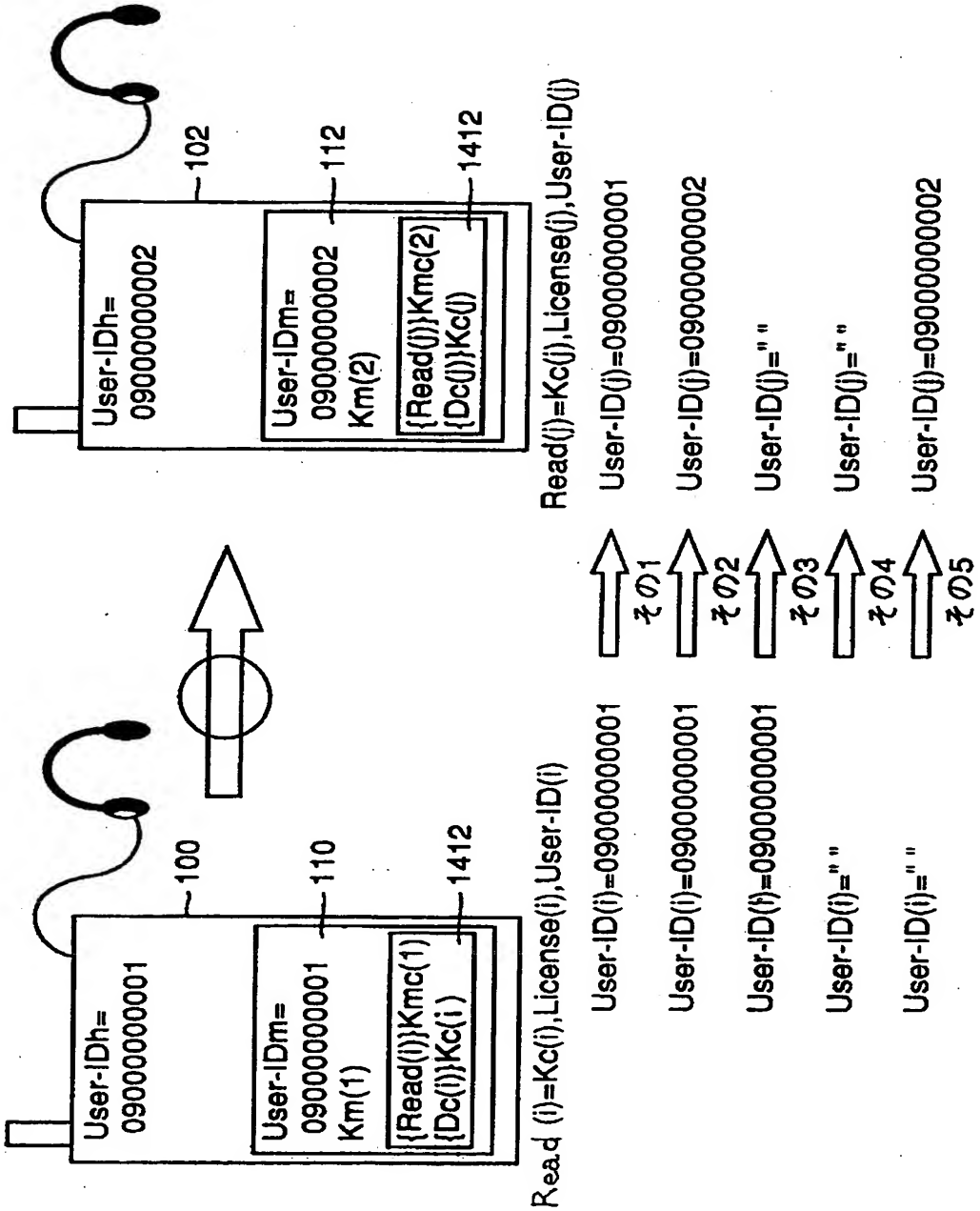
【図１６】


102
112
1412
User-IDh=
09000000002
User-IDm=
09000000002
Km(2)
{Read(j)}Kmc(2)
{Dc(j)}Kc(j)
100
110
1412
User-IDh=
09000000001
User-IDm=
09000000001
Km(1)
{Read(i)}Kmc(1)
{Dc(i)}Kc(i)
移動

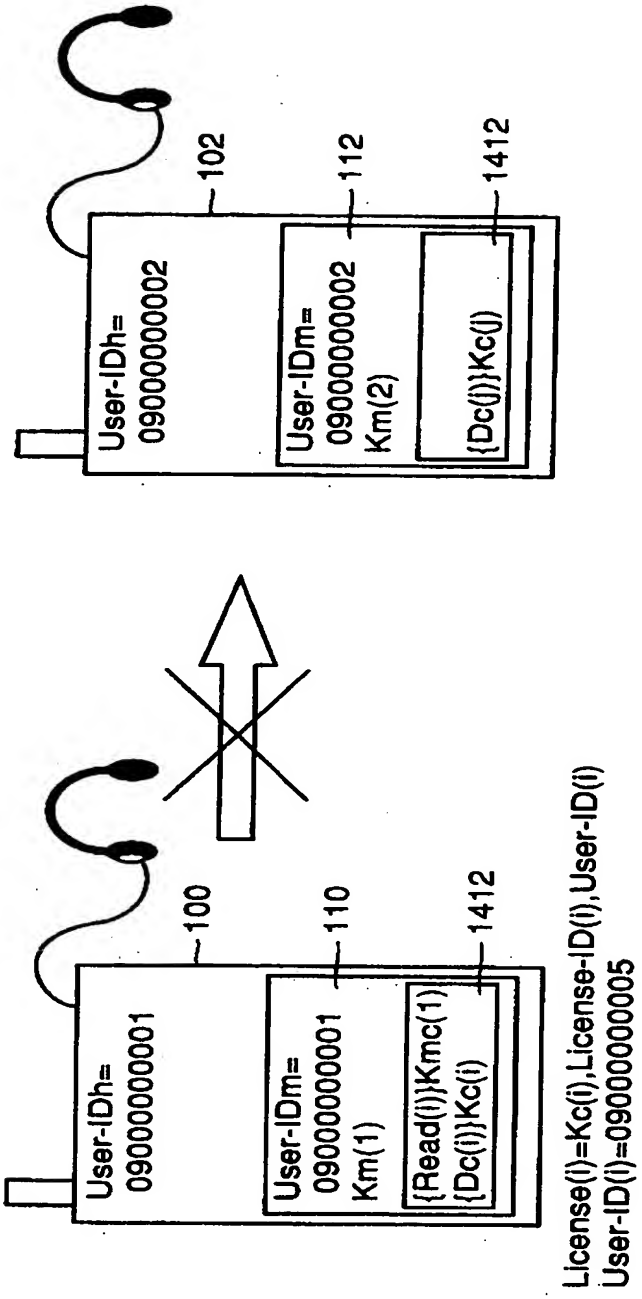
【図１７】


102
112
1412
User-IDh=
0900000002
User-IDm=
0900000002
Km(2)
{Dc(j)}Kc(j)
100
110
1412
User-IDh=
0900000001
User-IDm=
0900500001
Km(1)
{Read(i)}Kmc(1)
{Dc(i)}Kc(i)
移動

【図１８】


User-IDh=
09000000001
100
User-IDm=
09000000001
Km(1)
110
{Read(i)}Kmc(1)
{Dc(i)}Kc(i)
1412
Read (i)=Kc(i),License(i),User-ID(i)
User-IDh=
09000000002
102
User-IDm=
09000000002
Km(2)
112
{Read(j)}Kmc(2)
{Dc(j)}Kc(j)
1412
Read(j)=Kc(j),License(j),User-ID(j)
User-ID(i)=09000000001
User-ID(j)=09000000001
その1
User-ID(i)=09000000001
User-ID(j)=09000000002
その2
User-ID(i)=09000000001
User-ID(j)=""
その3
User-ID(i)=""
User-ID(j)=""
その4
User-ID(i)=""
User-ID(j)=09000000002
その5

【図１９】


102
112
1412
User-IDh=
09000000002
User-IDm=
09000000002
Km(2)
{Dc(j)}Kc(j)
100
110
1412
User-IDh=
09000000001
User-IDm=
09000000001
Km(1)
{Read(i)}Kmc(1)
{Dc(i)}Kc(i)
License(i)=Kc(i),License-ID(i),User-ID(i)
User-ID(i)=09000000005

【書類名】　　要約書

【要約】

【課題】　ユーザの許可なく配信データを消去、移動されることを防止することが可能な記録装置を提供する。

【解決手段】　メモリカード１１０は、メモリカードのユーザを識別するユーザＩＤデータを保持するユーザＩＤ保持部１５３０と、メモリカード１１０に対するアクセスを制限する第１の保守情報を保持する第１の保守情報保持部１５２０と、コンテンツデータごとのアクセスを制限する第２の保守情報を保持する第２の保守情報保持部１５４０とを備える。メモリカード１１０は、ユーザＩＤデータに基づいて、再生装置側のユーザを識別し、正規なユーザ以外が第１および第２の保守情報を変更することを禁じる。

【選択図】　　図２

認定・付加情報

特許出願の番号	平成１１年　特許願　第２４３７４１号
受付番号	５９９００８３８６５１
書類名	特許願
担当官	濱谷　よし子　　１６１４
作成日	平成１１年　９月　３日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000005223
- 【住所又は居所】 神奈川県川崎市中原区上小田中４丁目１番１号
- 【氏名又は名称】 富士通株式会社

【特許出願人】
- 【識別番号】 000005108
- 【住所又は居所】 東京都千代田区神田駿河台四丁目６番地
- 【氏名又は名称】 株式会社日立製作所

【特許出願人】
- 【識別番号】 000004167
- 【住所又は居所】 東京都港区赤坂４丁目１４番１４号
- 【氏名又は名称】 日本コロムビア株式会社

【特許出願人】
- 【識別番号】 000001889
- 【住所又は居所】 大阪府守口市京阪本通２丁目５番５号
- 【氏名又は名称】 三洋電機株式会社

【代理人】 申請人
- 【識別番号】 100064746
- 【住所又は居所】 大阪府大阪市北区南森町２丁目１番２９号　住友銀行南森町ビル　深見特許事務所
- 【氏名又は名称】 深見　久郎

【選任した代理人】
- 【識別番号】 100085132
- 【住所又は居所】 大阪府大阪市北区南森町２丁目１番２９号　住友銀行南森町ビル　深見特許事務所
- 【氏名又は名称】 森田　俊雄

【選任した代理人】
- 【識別番号】 100091409

次頁有

認定・付加情報（続き）

【住所又は居所】　大阪府大阪市北区南森町２－１－２９　住友銀行南森町ビル　深見特許事務所
【氏名又は名称】　伊藤　英彦
【選任した代理人】
【識別番号】　100096781
【住所又は居所】　大阪府大阪市北区南森町２－１－２９　住友銀行南森町ビル　深見特許事務所
【氏名又は名称】　堀井　豊

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所

出 願 人 履 歴 情 報

識別番号　〔０００００４１６７〕

１．変更年月日　１９９０年　８月２１日
［変更理由］　新規登録
住　所　東京都港区赤坂４丁目１４番１４号
氏　名　日本コロムビア株式会社

出願人履歴情報

識別番号　〔０００００１８８９〕

１．変更年月日　１９９３年１０月２０日
［変更理由］　住所変更
住　所　大阪府守口市京阪本通２丁目５番５号
氏　名　三洋電機株式会社